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

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

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

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
AC-02	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system;b. Assign account managers;c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;d. Specify:1. Authorized users of the system;2. Group and role membership; and3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];g. Monitor the use of accounts;h. Notify account managers and [Assignment: organization-defined personnel or roles] within:1. [Assignment: organization-defined time period] when accounts are no longer required;2. [Assignment: organization-defined time period] when users are terminated or transferred; and3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual;i. Authorize access to the system based on:1. A valid access authorization;2. Intended system usage; and3. [Assignment: organization-defined attributes (as required)];j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; andl. Align account management processes with personnel termination and transfer processes.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
AC-02	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system;b. Assign account managers;c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;d. Specify:1. Authorized users of the system;2. Group and role membership; and3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];g. Monitor the use of accounts;h. Notify account managers and [Assignment: organization-defined personnel or roles] within:1. [Assignment: organization-defined time period] when accounts are no longer required;2. [Assignment: organization-defined time period] when users are terminated or transferred; and3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual;i. Authorize access to the system based on:1. A valid access authorization;2. Intended system usage; and3. [Assignment: organization-defined attributes (as required)];j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; andl. Align account management processes with personnel termination and transfer processes.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	
AC-02(13)	Account Management | Disable Accounts for High-risk Individuals	Disable accounts of individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks].	Functional	Intersects With	High-Risk Terminations	HRS-09.2	Mechanisms exist to expedite the process of removing "high risk" individual's access to Technology Assets, Applications, Services and/or Data (TAASD) upon termination, as determined by management.	5	
AC-02(13)	Account Management | Disable Accounts for High-risk Individuals	Disable accounts of individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks].	Functional	Intersects With	Account Disabling for High Risk Individuals	IAC-15.6	Mechanisms exist to disable accounts immediately upon notification for users posing a significant risk to the organization.	5	
AC-03	Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
AC-03	Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	
AC-03	Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
AC-03(02)	Access Enforcement | Dual Authorization	Enforce dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined actions].	Functional	Intersects With	Two-Person Rule	HRS-12.1	Mechanisms exist to enforce a two-person rule for implementing changes to sensitive Technology Assets, Applications and/or Services (TAAS).	5	
AC-03(02)	Access Enforcement | Dual Authorization	Enforce dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined actions].	Functional	Intersects With	Dual Authorization for Privileged Commands	IAC-20.5	Automated mechanisms exist to enforce dual authorization for privileged commands.	5	
AC-03(14)	Access Enforcement | Individual Access	Provide [Assignment: organization-defined mechanisms] to enable individuals to have access to the following elements of their personally identifiable information: [Assignment: organization-defined elements].	Functional	Equal	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	10	
AC-05	Separation of Duties	a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; andb. Define system access authorizations to support separation of duties.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
AC-05	Separation of Duties	a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; andb. Define system access authorizations to support separation of duties.	Functional	Intersects With	Dual Authorization for Change	CHG-04.3	Mechanisms exist to enforce a two-person rule for implementing changes to critical Technology Assets, Applications and/or Services (TAAS).	5	
AC-05	Separation of Duties	a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; andb. Define system access authorizations to support separation of duties.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	
AC-05	Separation of Duties	a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; andb. Define system access authorizations to support separation of duties.	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	
AC-06	Least Privilege	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
AC-06	Least Privilege	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
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	
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	
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	
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	
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	
AC-23	Data Mining Protection	Employ [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to detect and protect against unauthorized data mining.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to: (1) The purpose(s) originally	5	
AT-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; andc. Review and update the current awareness and training:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
AT-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; andc. Review and update the current awareness and training:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
AT-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; andc. Review and update the current awareness and training:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
AT-02	Literacy Training and Awareness	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):1. As part of initial training for new users and [Assignment: organization-defined frequency] thereafter; and2. When required by system changes or following [Assignment: organization-defined events];b. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques];c. Update literacy training and awareness content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; andd. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.	Functional	Equal	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	10	
AT-03	Role-based Training	a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined roles and responsibilities]:1. Before authorizing access to the system, information, or performing assigned duties, and [Assignment: organization-defined frequency] thereafter; and2. When required by system changes;b. Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; andc. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
AT-03(05)	Role-based Training | Processing Personally Identifiable Information	Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of personally identifiable information processing and transparency controls.	Functional	Equal	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	10	
AT-04	Training Records	a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; andb. Retain individual training records for [Assignment: organization-defined time period].	Functional	Equal	Security, Compliance & Resilience Training Records	SAT-04	training activities, including: (1) Initial security, compliance and resilience awareness training; (2) Recurring awareness training; and (3) Technology Assets,	10	
AU-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; andc. Review and update the current audit and accountability:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
AU-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; andc. Review and update the current audit and accountability:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
AU-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; andc. Review and update the current audit and accountability:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
AU-02	Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-02a.) along with the frequency of (or situation requiring) logging for each identified event type];d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; ande. Review and update the event types selected for logging [Assignment: organization-defined frequency]	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
AU-02	Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-02a.) along with the frequency of (or situation requiring) logging for each identified event type];d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; ande. Review and update the event types selected for logging [Assignment: organization-defined frequency]	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
AU-03(03)	Content of Audit Records | Limit Personally Identifiable Information Elements	Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: [Assignment: organization-defined elements].	Functional	Equal	Limit Personal Data (PD) In Audit Records	MON-03.5	Mechanisms exist to limit Personal Data (PD) contained in audit records to the elements identified in the Data Privacy Risk Assessment (DPRA).	10	
AU-06	Audit Record Review, Analysis, and Reporting	a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity;b. Report findings to [Assignment: organization-defined personnel or roles]; andc. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
AU-06	Audit Record Review, Analysis, and Reporting	a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity;b. Report findings to [Assignment: organization-defined personnel or roles]; andc. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.	Functional	Intersects With	Audit Level Adjustments	MON-02.6	Mechanisms exist to adjust the level of audit review, analysis and reporting based on evolving threat information from law enforcement, industry associations or other credible sources of threat intelligence.	5	
AU-08	Time Stamps	a. Use internal system clocks to generate time stamps for audit records; andb. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.	Functional	Intersects With	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	5	
AU-08	Time Stamps	a. Use internal system clocks to generate time stamps for audit records; andb. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.	Functional	Intersects With	Time Stamps	MON-07	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to use an authoritative time source to generate time stamps for event logs.	5	
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	
CA-01	Policy and Procedures	[Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] assessment, authorization, and monitoring policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; andc. Review and update the current assessment, authorization, and monitoring:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
CA-01	Policy and Procedures	[Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] assessment, authorization, and monitoring policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; andc. Review and update the current assessment, authorization, and monitoring:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
CA-01	Policy and Procedures	[Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] assessment, authorization, and monitoring policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; andc. Review and update the current assessment, authorization, and monitoring:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
CA-02	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;b. Develop a control assessment plan that describes the scope of the assessment including:1. Controls and control enhancements under assessment;2. Assessment procedures to be used to determine control effectiveness; and3. Assessment environment, assessment team, and assessment roles and responsibilities;c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;d. Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;e. Produce a control assessment report that document the results of the assessment; andf. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	
CA-02	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;b. Develop a control assessment plan that describes the scope of the assessment including:1. Controls and control enhancements under assessment;2. Assessment procedures to be used to determine control effectiveness; and3. Assessment environment, assessment team, and assessment roles and responsibilities;c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;d. Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;e. Produce a control assessment report that document the results of the assessment; andf. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	5	
CA-02	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;b. Develop a control assessment plan that describes the scope of the assessment including:1. Controls and control enhancements under assessment;2. Assessment procedures to be used to determine control effectiveness; and3. Assessment environment, assessment team, and assessment roles and responsibilities;c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;d. Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;e. Produce a control assessment report that document the results of the assessment; andf. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
CA-02	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;b. Develop a control assessment plan that describes the scope of the assessment including:1. Controls and control enhancements under assessment;2. Assessment procedures to be used to determine control effectiveness; and3. Assessment environment, assessment team, and assessment roles and responsibilities;c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;d. Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;e. Produce a control assessment report that document the results of the assessment; andf. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
CA-02	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;b. Develop a control assessment plan that describes the scope of the assessment including:1. Controls and control enhancements under assessment;2. Assessment procedures to be used to determine control effectiveness; and3. Assessment environment, assessment team, and assessment roles and responsibilities;c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;d. Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;e. Produce a control assessment report that document the results of the assessment; andf. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
CA-05	Plan of Action and Milestones	a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; andb. Update existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g.	5	
CA-06	Authorization	a. Assign a senior official as the authorizing official for the system;b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;c. Ensure that the authorizing official for the system, before commencing operations:1. Accepts the use of common controls inherited by the system; and2. Authorizes the system to operate;d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;e. Update the authorizations [Assignment: organization-defined frequency].	Functional	Equal	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
CA-07	Continuous Monitoring	Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:a. Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics];b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness;c. Ongoing control assessments in accordance with the continuous monitoring strategy;d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;e. Correlation and analysis of information generated by control assessments and monitoring;f. Response actions to address results of the analysis of control assessment and monitoring information; andg. Reporting the security and privacy status of the system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
CA-07(01)	Continuous Monitoring | Independent Assessment	Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.	Functional	Intersects With	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant	5	
CA-07(01)	Continuous Monitoring | Types of Assessments	Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
CA-07(04)	Continuous Monitoring | Risk Monitoring	Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:a. Effectiveness monitoring;b. Compliance monitoring; andc. Change monitoring.	Functional	Equal	Risk Monitoring	RSK-11	Mechanisms exist to ensure risk monitoring as an integral part of the continuous monitoring strategy that includes monitoring the effectiveness of security, compliance and resilience controls, compliance and change management.	10	
CM-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; andc. Review and update the current configuration management:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
CM-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; andc. Review and update the current configuration management:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
CM-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; andc. Review and update the current configuration management:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
CM-02	Baseline Configuration	a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; andb. Review and update the baseline configuration of the system:1. [Assignment: organization-defined frequency];2. When required due to [Assignment: organization-defined circumstances]; and3. When system components are installed or upgraded.	Functional	Intersects With	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	
CM-02	Baseline Configuration	a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; andb. Review and update the baseline configuration of the system:1. [Assignment: organization-defined frequency];2. When required due to [Assignment: organization-defined circumstances]; and3. When system components are installed or upgraded.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
CM-03	Configuration Change Control	b. Determine and document the types of changes to the system that are configuration-controlled;b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;c. Document configuration change decisions associated with the system;d. Implement approved configuration-controlled changes to the system;e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period];f. Monitor and review activities associated with configuration-controlled changes to the system; andg. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined configuration	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
CM-03	Configuration Change Control	b. Determine and document the types of changes to the system that are configuration-controlled;b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;c. Document configuration change decisions associated with the system;d. Implement approved configuration-controlled changes to the system;e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period];f. Monitor and review activities associated with configuration-controlled changes to the system; andg. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined configuration	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
CM-03(02)	Configuration Change Control | Testing, Validation, and Documentation of Changes	Test, validate, and document changes to the system before finalizing the implementation of the changes.	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	5	
CM-03(02)	Configuration Change Control | Testing, Validation, and Documentation of Changes	Test, validate, and document changes to the system before finalizing the implementation of the changes.	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	5	
CM-04	Impact Analyses	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.	Functional	Equal	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	10	
CM-05	Access Restrictions for Change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.	Functional	Intersects With	Governing Access Restriction for Change	END-03.2	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to Technology Assets, Applications and/or Services (TAAS).	5	
CM-05	Access Restrictions for Change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
CM-06	Configuration Settings	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations];b. Implement the configuration settings;c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; andd. Monitor and control changes to the configuration settings in accordance with organizational policies and	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
CM-06	Configuration Settings	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations];b. Implement the configuration settings;c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; andd. Monitor and control changes to the configuration settings in accordance with organizational policies and	Functional	Intersects With	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	5	
CM-07(02)	Least Functionality | Prevent Program Execution	Prevent program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].	Functional	Intersects With	Prevent Program Execution	SEA-06	Automated mechanisms exist to prevent the execution of unauthorized software programs.	5	
CM-07(02)	Least Functionality | Prevent Program Execution	Prevent program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].	Functional	Intersects With	Prevent Unauthorized Software Execution	CFG-03.2	Mechanisms exist to configure systems to prevent the execution of unauthorized software programs.	5	
CM-08	System Component Inventory	a. Develop and document an inventory of system components that:1. Accurately reflects the system;2. Includes all components within the system;3. Does not include duplicate accounting of components or components assigned to any other system;4. Is at the level of granularity deemed necessary for tracking and reporting; and5. Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; andb. Review and update the system component inventory [Assignment: organization-defined frequency].	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
CM-08	System Component Inventory	a. Develop and document an inventory of system components that:1. Accurately reflects the system;2. Includes all components within the system;3. Does not include duplicate accounting of components or components assigned to any other system;4. Is at the level of granularity deemed necessary for tracking and reporting; and5. Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; andb. Review and update the system component inventory [Assignment: organization-defined frequency].	Functional	Intersects With	Component Duplication Avoidance	AST-02.3	Mechanisms exist to establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components that prevents assets from being duplicated in other asset inventories.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
CM-08(03)	System Component Inventory | Automated Unauthorized Component Detection	a. Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; andb. Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].	Functional	Intersects With	Automated Unauthorized Component Detection	AST-02.2	Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.	5	
CM-08(03)	System Component Inventory | Automated Unauthorized Component Detection	a. Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; andb. Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].	Functional	Intersects With	Software Installation Alerts	END-03.1	Mechanisms exist to generate an alert when new software is detected.	5	
CM-08(03)	System Component Inventory | Automated Unauthorized Component Detection	a. Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; andb. Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].	Functional	Intersects With	Unauthorized Installation Alerts	CFG-05.1	Mechanisms exist to configure systems to generate an alert when the unauthorized installation of software is detected.	5	
CM-09	Configuration Management Plan	Develop, document, and implement a configuration management plan for the system that:a. Addresses roles, responsibilities, and configuration management processes and procedures;b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;c. Defines the configuration items for the system and places the configuration items under configuration management;d. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; ande. Protects the configuration management plan from unauthorized disclosure and modification.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
CM-09	Configuration Management Plan	Develop, document, and implement a configuration management plan for the system that:a. Addresses roles, responsibilities, and configuration management processes and procedures;b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;c. Defines the configuration items for the system and places the configuration items under configuration management;d. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; ande. Protects the configuration management plan from unauthorized disclosure and modification.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5	
CM-11	User-installed Software	a. Establish [Assignment: organization-defined policies] governing the installation of software by users;b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; andc. Monitor policy compliance [Assignment: organization-defined frequency].	Functional	Intersects With	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	5	
CM-11	User-installed Software	a. Establish [Assignment: organization-defined policies] governing the installation of software by users;b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; andc. Monitor policy compliance [Assignment: organization-defined frequency].	Functional	Intersects With	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5	
CM-11(02)	User-installed Software | Software Installation with Privileged Status	Allow user installation of software only with explicit privileged status.	Functional	Intersects With	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5	
CM-11(02)	User-installed Software | Software Installation with Privileged Status	Allow user installation of software only with explicit privileged status.	Functional	Intersects With	Restrict Roles Permitted To Install Software	CFG-05.2	Mechanisms exist to configure systems to prevent the installation of software, unless the action is performed by a privileged user or service.	5	
CM-11(02)	User-installed Software | Software Installation with Privileged Status	Allow user installation of software only with explicit privileged status.	Functional	Intersects With	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	5	
CM-11(03)	User-installed Software | Automated Enforcement and Monitoring	Enforce and monitor compliance with software installation policies using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.	5	
CM-11(03)	User-installed Software | Automated Enforcement and Monitoring	Enforce and monitor compliance with software installation policies using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Integrity Assurance & Enforcement (IAE)	CFG-06.1	Automated mechanisms exist to identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the unauthorized change.	5	
CM-11(03)	User-installed Software | Automated Enforcement and Monitoring	Enforce and monitor compliance with software installation policies using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Software Installation Alerts	END-03.1	Mechanisms exist to generate an alert when new software is detected.	5	
CM-11(03)	User-installed Software | Automated Enforcement and Monitoring	Enforce and monitor compliance with software installation policies using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Unauthorized Installation Alerts	CFG-05.1	Mechanisms exist to configure systems to generate an alert when the unauthorized installation of software is detected.	5	
CP-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; andc. Review and update the current contingency planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
CP-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; andc. Review and update the current contingency planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
CP-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; andc. Review and update the current contingency planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
CP-02	Contingency Plan	Identifies essential mission and business functions and associated contingency requirements;2. Provides recovery objectives, restoration priorities, and metrics;3. Addresses contingency roles, responsibilities, assigned individuals with contact information;4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;6. Addresses the sharing of contingency information; and7. Is reviewed and approved by [Assignment: organization-defined personnel or roles];b. Distribute copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];c. Coordinate contingency planning activities with incident handling activities;d. Review the contingency plan for the system [Assignment: organization-defined frequency];e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;f. Communicate contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; andh. Protect the contingency plan from	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
CP-02	Contingency Plan	Identifies essential mission and business functions and associated contingency requirements;2. Provides recovery objectives, restoration priorities, and metrics;3. Addresses contingency roles, responsibilities, assigned individuals with contact information;4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;6. Addresses the sharing of contingency information; and7. Is reviewed and approved by [Assignment: organization-defined personnel or roles];b. Distribute copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];c. Coordinate contingency planning activities with incident handling activities;d. Review the contingency plan for the system [Assignment: organization-defined frequency];e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;f. Communicate contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; andh. Protect the contingency plan from	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	
CP-02(03)	Contingency Plan | Resume Mission and Business Functions	Plan for the resumption of [Selection (one): all; essential] mission and business functions within [Assignment: organization-defined time period] of contingency plan activation.	Functional	Intersects With	Resume All Missions & Business Functions	BCD-02.1	Mechanisms exist to resume all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation.	5	
CP-02(03)	Contingency Plan | Resume Mission and Business Functions	Plan for the resumption of [Selection (one): all; essential] mission and business functions within [Assignment: organization-defined time period] of contingency plan activation.	Functional	Intersects With	Resume Essential Missions & Business Functions	BCD-02.3	Mechanisms exist to resume essential missions and business functions within an organization-defined time period of contingency plan activation.	5	
CP-04	Contingency Plan Testing	a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests].b. Review the contingency plan test results; andc. Initiate corrective actions, if needed.	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5	
CP-04	Contingency Plan Testing	a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests].b. Review the contingency plan test results; andc. Initiate corrective actions, if needed.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
CP-10	System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.	Functional	Intersects With	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
CP-10	System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
CP-10	System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
IA-01	Policy and Procedures	[Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; andc. Review and update the current identification and authentication:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
IA-01	Policy and Procedures	[Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; andc. Review and update the current identification and authentication:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
IA-01	Policy and Procedures	[Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; andc. Review and update the current identification and authentication:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
IA-02(01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	5	
IA-02(01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Local Access to Privileged Accounts	IAC-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	5	
IA-02(01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Information Assurance Enabled Products	TDA-02.2	Mechanisms exist to limit the use of commercially-provided Information Assurance (IA) and IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated or NSA-approved.	5	
IA-02(01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Out-of-Band Multi-Factor Authentication	IAC-06.4	Mechanisms exist to implement Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.	5	
IA-02(01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5	
IA-02(01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Network Access to Non-Privileged Accounts	IAC-06.2	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
IA-02(01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Hardware Token-Based Authentication	IAC-10.7	Automated mechanisms exist to ensure organization-defined token quality requirements are satisfied for hardware token-based authentication.	5	
IA-02(02)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Information Assurance Enabled Products	TDA-02.2	Mechanisms exist to limit the use of commercially-provided Information Assurance (IA) and IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated or NSA-approved.	5	
IA-02(02)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Network Access to Non-Privileged Accounts	IAC-06.2	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts.	5	
IA-02(02)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Out-of-Band Multi-Factor Authentication	IAC-06.4	Mechanisms exist to implement Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.	5	
IA-02(02)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Hardware Token-Based Authentication	IAC-10.7	Automated mechanisms exist to ensure organization-defined token quality requirements are satisfied for hardware token-based authentication.	5	
IA-02(02)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5	
IA-02(02)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	5	
IA-02(02)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Local Access to Privileged Accounts	IAC-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	5	
IA-03(04)	Device Identification and Authentication | Device Attestation	Handle device identification and authentication based on attestation by [Assignment: organization-defined configuration management process].	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	5	
IA-03(04)	Device Identification and Authentication | Device Attestation	Handle device identification and authentication based on attestation by [Assignment: organization-defined configuration management process].	Functional	Intersects With	Device Attestation	IAC-04.1	Mechanisms exist to ensure device identification and authentication is accurate by centrally-managing the joining of systems to the domain as part of the initial asset configuration management process.	5	
IA-04	Identifier Management	Manage system identifiers by:a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier;b. Selecting an identifier that identifies an individual, group, role, service, or device;c. Assigning the identifier to the intended individual, group, role, service, or device; andd. Preventing reuse of identifiers for [Assignment: organization-defined time period]	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
IA-04	Identifier Management	Manage system identifiers by:a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier;b. Selecting an identifier that identifies an individual, group, role, service, or device;c. Assigning the identifier to the intended individual, group, role, service, or device; andd. Preventing reuse of identifiers for [Assignment: organization-defined time period]	Functional	Intersects With	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).	5	
IA-04(04)	Identifier Management | Identify User Status	Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
IA-04(04)	Identifier Management | Identify User Status	Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].	Functional	Intersects With	User Identity (ID) Management	IAC-09.1	Mechanisms exist to ensure proper user identification management for non-consumer users and administrators.	5	
IA-04(04)	Identifier Management | Identify User Status	Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].	Functional	Intersects With	Identity User Status	IAC-09.2	Mechanisms exist to identify contractors and other third-party users through unique username characteristics.	5	
IA-05	Authenticator Management	Manage system authenticators by:a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;b. Establishing initial authenticator content for any authenticators issued by the organization;c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;e. Changing default authenticators prior to first use;f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur;g. Protecting authenticator content from unauthorized disclosure and modification;h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; andi. Changing authenticators for group or role accounts when membership to those accounts changes	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
IA-05	Authenticator Management	Manage system authenticators by:a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;b. Establishing initial authenticator content for any authenticators issued by the organization;c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;e. Changing default authenticators prior to first use;f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur;g. Protecting authenticator content from unauthorized disclosure and modification;h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; andi. Changing authenticators for group or role accounts when membership to those accounts changes.	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	
IA-05(01)	Authenticator Management | Password-based Authentication	For password-based authentication:a. Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);c. Transmit passwords only over cryptographically-protected channels;d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;e. Require immediate selection of a new password upon account recovery;f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;g. Employ automated tools to assist the user in selecting strong password authenticators; andh. Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].	Functional	Intersects With	Automated Support For Password Strength	IAC-10.4	Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.	5	
IA-05(01)	Authenticator Management | Password-based Authentication	For password-based authentication:a. Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);c. Transmit passwords only over cryptographically-protected channels;d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;e. Require immediate selection of a new password upon account recovery;f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;g. Employ automated tools to assist the user in selecting strong password authenticators; andh. Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
IA-05(01)	Authenticator Management | Password-based Authentication	For password-based authentication:a. Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);c. Transmit passwords only over cryptographically-protected channels;d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;e. Require immediate selection of a new password upon account recovery;f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;g. Employ automated tools to assist the user in selecting strong password authenticators; andh. Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
IA-05(02)	Authenticator Management | Public Key-based Authentication	a. For public key-based authentication:1. Enforce authorized access to the corresponding private key; and2. Map the authenticated identity to the account of the individual or group; andb. When public key infrastructure (PKI) is used:1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and2. Implement a local cache of revocation data to support path discovery and validation.	Functional	Equal	PKI-Based Authentication	IAC-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	10	
IA-05(06)	Authenticator Management | Protection of Authenticators	Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.	Functional	Intersects With	User Responsibilities for Account Management	IAC-18	Mechanisms exist to compel users to follow accepted practices in the use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards, certificates, etc.).	5	
IA-05(06)	Authenticator Management | Protection of Authenticators	Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
IA-05(08)	Authenticator Management | Multiple System Accounts	Implement [Assignment: organization-defined security controls] to manage the risk of compromise due to individuals having accounts on multiple systems.	Functional	Intersects With	Multiple System Accounts	IAC-10.9	Mechanisms exist to implement security safeguards to manage the risk of compromise due to individuals having accounts on multiple Technology Assets, Applications and/or Services (TAAS).	5	
IA-05(08)	Authenticator Management | Multiple System Accounts	Implement [Assignment: organization-defined security controls] to manage the risk of compromise due to individuals having accounts on multiple systems.	Functional	Intersects With	Privileged Account Identifiers	IAC-09.5	Mechanisms exist to uniquely manage privileged accounts to identify the account as a privileged user or service.	5	
IA-07	Cryptographic Module Authentication	Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.	Functional	Intersects With	Cryptographic Module Authentication	IAC-12	Mechanisms exist to ensure cryptographic modules adhere to applicable statutory, regulatory and contractual requirements for security strength.	5	
IA-07	Cryptographic Module Authentication	Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.	Functional	Intersects With	Automated Authentication Through Cryptographic Modules	CRY-02	Automated mechanisms exist to enable systems to authenticate to a cryptographic module.	5	
IA-12(04)	Identity Proofing | In-person Validation and Verification	Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
IA-12(04)	Identity Proofing | In-person Validation and Verification	Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.	Functional	Intersects With	In-Person or Trusted Third-Party Registration	IAC-10.3	Mechanisms exist to conduct in-person or trusted third-party identify verification before user accounts for third-parties are created.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
IA-12(04)	Identity Proofing | In-person Validation and Verification	Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.	Functional	Intersects With	In-Person Validation & Verification	IAC-28.4	Mechanisms exist to require that the validation and verification of identity evidence be conducted in person before a designated registration authority.	5	
IR-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; andc. Review and update the current incident response:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
IR-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; andc. Review and update the current incident response:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
IR-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; andc. Review and update the current incident response:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	5	
IR-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; andc. Review and update the current incident response:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5	
IR-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; andc. Review and update the current incident response:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
IR-02	Incident Response Training	a. Provide incident response training to system users consistent with assigned roles and responsibilities:1. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access;2. When required by system changes; and3. [Assignment: organization-defined frequency] thereafter; andb. Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5	
IR-02(03)	Incident Response Training | Breach	Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5	
IR-03	Incident Response Testing	Test the effectiveness of the incident response capability for the system [Assignment: organization-defined frequency] using the following tests: [Assignment: organization-defined tests].	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
IR-04	Incident Handling	a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;b. Coordinate incident handling activities with contingency planning activities;c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; andd. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.	Functional	Equal	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
IR-04(03)	Incident Handling | Continuity of Operations	Identify [Assignment: organization-defined classes of incidents] and take the following actions in response to those incidents to ensure continuation of organizational mission and business functions: [Assignment: organization-defined actions to take in response to classes of incidents].	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
IR-04(03)	Incident Handling | Continuity of Operations	Identify [Assignment: organization-defined classes of incidents] and take the following actions in response to those incidents to ensure continuation of organizational mission and business functions: [Assignment: organization-defined actions to take in response to classes of incidents].	Functional	Intersects With	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	5	
IR-04(04)	Incident Handling | Information Correlation	Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
IR-04(04)	Incident Handling | Information Correlation	Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
IR-04(05)	Incident Handling | Automatic Disabling of System	Implement a configurable capability to automatically disable the system if [Assignment: organization-defined security violations] are detected.	Functional	Intersects With	Automated Response to Suspicious Events	MON-01.11	Automated mechanisms exist to implement pre-determined corrective actions in response to detected events that have security incident implications.	5	
IR-04(05)	Incident Handling | Automatic Disabling of System	Implement a configurable capability to automatically disable the system if [Assignment: organization-defined security violations] are detected.	Functional	Intersects With	Automatic Disabling of Technology Assets, Applications and/or Services (TAAS)	IRO-02.6	Mechanisms exist to automatically disable Technology Assets, Applications and/or Services (TAAS), upon detection of a possible incident that meets organizational criteria, which allows for forensic analysis to be	5	
IR-04(10)	Incident Handling | Supply Chain Coordination	Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5	
IR-04(10)	Incident Handling | Supply Chain Coordination	Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.	Functional	Intersects With	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity and data protection incident information to the provider of the Technology Assets, Applications and/or Services (TAAS) and other organizations involved in the supply chain for TAAS related to	5	
IR-04(12)	Incident Handling | Malicious Code and Forensic Analysis	Analyze malicious code and/or other residual artifacts remaining in the system after the incident.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5	
IR-04(12)	Incident Handling | Malicious Code and Forensic Analysis	Analyze malicious code and/or other residual artifacts remaining in the system after the incident.	Functional	Intersects With	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	5	
IR-04(13)	Incident Handling | Behavior Analysis	Analyze anomalous or suspected adversarial behavior in or related to [Assignment: organization-defined environments or resources].	Functional	Intersects With	Honeypots	SEA-11	Mechanisms exist to utilize honeypots that are specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting and analyzing such attacks.	5	
IR-04(13)	Incident Handling | Behavior Analysis	Analyze anomalous or suspected adversarial behavior in or related to [Assignment: organization-defined environments or resources].	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
IR-04(13)	Incident Handling | Behavior Analysis	Analyze anomalous or suspected adversarial behavior in or related to [Assignment: organization-defined environments or resources].	Functional	Intersects With	Honeyclients	SEA-12	Mechanisms exist to utilize honeyclients that proactively seek to identify malicious websites and/or web-based malicious code.	5	
IR-05	Incident Monitoring	Track and document incidents.	Functional	Equal	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	10	
IR-06	Incident Reporting	a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; andb. Report incident information to [Assignment: organization-defined authorities].	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
IR-06	Incident Reporting	a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; andb. Report incident information to [Assignment: organization-defined authorities].	Functional	Intersects With	Regulatory & Law Enforcement Contacts	IRO-14	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.	5	
IR-06	Incident Reporting	a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; andb. Report incident information to [Assignment: organization-defined authorities].	Functional	Intersects With	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	5	
IR-06(02)	Incident Reporting | Vulnerabilities Related to Incidents	Report system vulnerabilities associated with reported incidents to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5	
IR-06(02)	Incident Reporting | Vulnerabilities Related to Incidents	Report system vulnerabilities associated with reported incidents to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Vulnerabilities Related To Incidents	IRO-10.3	Mechanisms exist to report system vulnerabilities associated with reported cybersecurity and data protection incidents to organization-defined personnel or roles.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Relationship	Notes
IR-07	Incident Response Assistance	Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.	Functional	Equal	Incident Reporting Assistance	IRO-11	Mechanisms exist to provide incident response advice and assistance to users of Technology Assets, Applications and/or Services (TAAS) for the handling and reporting of actual and potential cybersecurity and data protection incidents.	10	
IR-08	Incident Response Plan	a. Develop an incident response plan that:1. Provides the organization with a roadmap for implementing its incident response capability;2. Describes the structure and organization of the incident response capability;3. Provides a high-level approach for how the incident response capability fits into the overall organization;4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;5. Defines reportable incidents;6. Provides metrics for measuring the incident response capability within the organization;7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;8. Addresses the sharing of incident information;9. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]; and10. Explicitly designates responsibility for incident response to [Assignment: organization-defined entities, personnel, or roles].b. Distribute copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements];c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;d. Communicate incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; ande. Protect the incident response plan from unauthorized disclosure and modification.	Functional	Equal	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	10	
IR-08(01)	Incident Response Plan | Breaches	Include the following in the Incident Response Plan for breaches involving personally identifiable information:a. A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;b. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; andc. Identification of applicable privacy requirements.	Functional	Equal	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
IR-09	Information Spillage Response	Respond to information spills by:a. Assigning [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills;b. Identifying the specific information involved in the system contamination;c. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill;d. Isolating the contaminated system or system component;e. Eradicating the information from the contaminated system or component;f. Identifying other systems or system components that may have been subsequently contaminated; andg. Performing the following additional actions: [Assignment: organization-defined actions]	Functional	Intersects With	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive/regulated data spills.	5	
IR-09	Information Spillage Response	Respond to information spills by:a. Assigning [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills;b. Identifying the specific information involved in the system contamination;c. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill;d. Isolating the contaminated system or system component;e. Eradicating the information from the contaminated system or component;f. Identifying other systems or system components that may have been subsequently contaminated; andg. Performing the following additional actions: [Assignment: organization-defined actions]	Functional	Intersects With	Sensitive / Regulated Data Spill Responsible Personnel	IRO-12.1	Mechanisms exist to formally assign personnel or roles with responsibility for responding to sensitive/regulated data spills.	5	
MA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; andc. Review and update the current maintenance:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	10	
MA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; andc. Review and update the current maintenance:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Remote Maintenance Notifications	MNT-05.2	Mechanisms exist to require maintenance personnel to notify affected stakeholders when remote, non-local maintenance is planned (e.g., date/time).	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
MA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; andc. Review and update the current maintenance:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	5	
MA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; andc. Review and update the current maintenance:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
MA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; andc. Review and update the current maintenance:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
MA-04	Nonlocal Maintenance	a. Approve and monitor nonlocal maintenance and diagnostic activities;b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;d. Maintain records for nonlocal maintenance and diagnostic activities; ande. Terminate session and network connections when nonlocal maintenance is completed.	Functional	Intersects With	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	5	
MA-04	Nonlocal Maintenance	a. Approve and monitor nonlocal maintenance and diagnostic activities;b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;d. Maintain records for nonlocal maintenance and diagnostic activities; ande. Terminate session and network connections when nonlocal maintenance is completed.	Functional	Intersects With	Remote Maintenance Notifications	MNT-05.2	Mechanisms exist to require maintenance personnel to notify affected stakeholders when remote, non-local maintenance is planned (e.g., date/time).	5	
MA-04	Nonlocal Maintenance	a. Approve and monitor nonlocal maintenance and diagnostic activities;b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;d. Maintain records for nonlocal maintenance and diagnostic activities; ande. Terminate session and network connections when nonlocal maintenance is completed.	Functional	Intersects With	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	5	
MP-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] media protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures; andc. Review and update the current media protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
MP-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] media protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures; andc. Review and update the current media protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
MP-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] media protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures; andc. Review and update the current media protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
MP-02	Media Access	Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	5	
MP-02	Media Access	Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM)	5	
MP-03	Media Marking	a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; andb. Exempt [Assignment: organization-defined types of system media] from marking if the media remain within [Assignment: organization-defined controlled areas].	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
MP-03	Media Marking	a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; andb. Exempt [Assignment: organization-defined types of system media] from marking if the media remain within [Assignment: organization-defined controlled areas].	Functional	Intersects With	Automated Marking	DCH-04.1	Automated mechanisms exist to mark physical media and digital files to indicate the distribution limitations, handling requirements and applicable security markings (if any) of the information to aid Data Loss Prevention (DLP) technologies.	5	
MP-06	Media Sanitization	a. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; andb. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
MP-06	Media Sanitization	a. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; andb. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
MP-06	Media Sanitization	a. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; andb. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	Functional	Intersects With	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).	5	
MP-06(03)	Media Sanitization | Nondestructive Techniques	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	
MP-06(03)	Media Sanitization | Nondestructive Techniques	Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices].	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
MP-06(03)	Media Sanitization | Nondestructive Techniques	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	
MP-07	Media Use	a. [Selection (one): Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; andb. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
MP-07	Media Use	a. [Selection (one): Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; andb. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.	Functional	Intersects With	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5	
MP-07	Media Use	a. [Selection (one): Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; andb. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.	Functional	Intersects With	Prohibit Use Without Owner	DCH-10.2	Mechanisms exist to prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.	5	
PE-01	Policy and Procedures	[Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; andc. Review and update the current physical and environmental protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
PE-01	Policy and Procedures	[Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; andc. Review and update the current physical and environmental protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
PE-01	Policy and Procedures	[Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; andc. Review and update the current physical and environmental protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
PE-08(03)	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	
PE-13(02)	Fire Protection | Suppression Systems — Automatic Activation and Notification	a. Employ fire suppression systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders]; andb. Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.	Functional	Intersects With	Automatic Fire Suppression	PES-08.3	Facility security mechanisms exist to employ an automatic fire suppression capability for critical systems when the facility is not staffed on a continuous basis.	5	
PE-13(02)	Fire Protection | Suppression Systems — Automatic Activation and Notification	a. Employ fire suppression systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders]; andb. Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.	Functional	Intersects With	Fire Suppression Devices	PES-08.2	Facility security mechanisms exist to utilize fire suppression devices/systems that provide automatic notification of any activation to organizational personnel and emergency	5	
PE-22	Component Marking	Mark [Assignment: organization-defined system hardware components] indicating the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-	5	
PE-22	Component Marking	Mark [Assignment: organization-defined system hardware components] indicating the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.	Functional	Intersects With	Component Marking	PES-16	Physical security mechanisms exist to mark system hardware components indicating the impact or classification level of the information permitted to be processed, stored or transmitted by the hardware component.	5	
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	
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	
PE-23	Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; andb. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.	Functional	Intersects With	Alternate Storage Site	BCD-08	Mechanisms exist to establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup information.	5	
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	
PE-23	Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; andb. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	
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	
PL-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; andc. Review and update the current planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
PL-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; andc. Review and update the current planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and	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	
PL-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; andc. Review and update the current planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and	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	
PL-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; andc. Review and update the current planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
PL-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; andc. Review and update the current planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
PL-02	System Security and Privacy Plans	enterprise architecture;2. Explicitly define the constituent system components;3. Describe the operational context of the system in terms of mission and business processes;4. Identify the individuals that fulfill system roles and responsibilities;5. Identify the information types processed, stored, and transmitted by the system;6. Provide the security categorization of the system, including supporting rationale;7. Describe any specific threats to the system that are of concern to the organization;8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;10. Provide an overview of the security and privacy requirements for the system;11. Identify any relevant control baselines or overlays, if applicable;12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;13. Include risk determinations for security and privacy architecture and design decisions;14. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; and15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles];c. Review the plans [Assignment: organization-defined frequency];d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments;	Functional	Intersects With	Plan / Coordinate with Other Organizational Entities	IAO-03.1	Mechanisms exist to plan and coordinate Information Assurance Program (IAP) activities with affected stakeholders before conducting such activities in order to reduce the potential impact on operations.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
PL-02	System Security and Privacy Plans	enterprise architecture;2. Explicitly define the constituent system components;3. Describe the operational context of the system in terms of mission and business processes;4. Identify the individuals that fulfill system roles and responsibilities;5. Identify the information types processed, stored, and transmitted by the system;6. Provide the security categorization of the system, including supporting rationale;7. Describe any specific threats to the system that are of concern to the organization;8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;10. Provide an overview of the security and privacy requirements for the system;11. Identify any relevant control baselines or overlays, if applicable;12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;13. Include risk determinations for security and privacy architecture and design decisions;14. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; and15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles];c. Review the plans [Assignment: organization-defined frequency];d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments;	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5	
PL-02	System Security and Privacy Plans	enterprise architecture;2. Explicitly define the constituent system components;3. Describe the operational context of the system in terms of mission and business processes;4. Identify the individuals that fulfill system roles and responsibilities;5. Identify the information types processed, stored, and transmitted by the system;6. Provide the security categorization of the system, including supporting rationale;7. Describe any specific threats to the system that are of concern to the organization;8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;10. Provide an overview of the security and privacy requirements for the system;11. Identify any relevant control baselines or overlays, if applicable;12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;13. Include risk determinations for security and privacy architecture and design decisions;14. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; and15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles];c. Review the plans [Assignment: organization-defined frequency];d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments;	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	5	
PL-04	Rules of Behavior	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;c. Review and update the rules of behavior [Assignment: organization-defined frequency]; andd. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more): [Assignment: organization-defined frequency]; when the rules are revised or updated]	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	5	
PL-04	Rules of Behavior	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;c. Review and update the rules of behavior [Assignment: organization-defined frequency]; andd. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more): [Assignment: organization-defined frequency]; when the rules are revised or updated]	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
PL-04	Rules of Behavior	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;c. Review and update the rules of behavior [Assignment: organization-defined frequency]; andd. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more): [Assignment: organization-defined frequency]; when the rules are revised or updated]	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	5	
PL-04(01)	Rules of Behavior | Social Media and External Site/application Usage Restrictions	Include in the rules of behavior, restrictions on:a. Use of social media, social networking sites, and external sites/applications;b. Posting organizational information on public websites; andc. Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.	Functional	Equal	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	10	
PL-08	Security and Privacy Architectures	system that:1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;3. Describe how the architectures are integrated into and support the enterprise architecture; and4. Describe any assumptions about, and dependencies on, external systems and services;b. Review and update the architectures [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture; andc. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
PL-09	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	Centralized Management of Security, Compliance & Resilience Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of security, compliance and resilience controls and related processes.	5	
PL-09	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	
PL-09	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
PL-09	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	Centralized Management of Antimalware Technologies	END-04.3	Mechanisms exist to centrally-manage antimalware technologies.	5	
PL-09	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	Central Management	END-08.1	Mechanisms exist to centrally-manage anti-phishing and spam protection technologies.	5	
PL-09	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	Centralized Management of Event Log Content	MON-03.6	Mechanisms exist to centrally manage and update the criteria to be captured in event logs generated by organization-defined system components.	5	
PM-01	Information Security Program Plan	a. Develop and disseminate an organization-wide information security program plan that:1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;3. Reflects the coordination among organizational entities responsible for information security; and4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;b. Review and update the organization-wide information security program plan [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; andc. Protect the information security program plan from unauthorized disclosure and modification.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
PM-01	Information Security Program Plan	a. Develop and disseminate an organization-wide information security program plan that:1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;3. Reflects the coordination among organizational entities responsible for information security; and4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;b. Review and update the organization-wide information security program plan [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; andc. Protect the information security program plan from unauthorized disclosure and modification.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
PM-01	Information Security Program Plan	a. Develop and disseminate an organization-wide information security program plan that:1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;3. Reflects the coordination among organizational entities responsible for information security; and4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;b. Review and update the organization-wide information security program plan [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; andc. Protect the information security program plan from unauthorized disclosure and modification.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
PM-03	Information Security and Privacy Resources	a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement;b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; andc. Make available for expenditure, the planned information security and privacy resources.	Functional	Equal	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	10	
PM-04	Plan of Action and Milestones Process	a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems:1. Are developed and maintained;2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and3. Are reported in accordance with established reporting requirements.b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
PM-04	Plan of Action and Milestones Process	a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems:1. Are developed and maintained;2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and3. Are reported in accordance with established reporting requirements.b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	(2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
PM-05	System Inventory	Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
PM-05	System Inventory	Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
PM-05(01)	System Inventory | Inventory of Personally Identifiable Information	Establish, maintain, and update [Assignment: organization-defined frequency] an inventory of all systems, applications, and projects that process personally identifiable information.	Functional	Intersects With	Inventory of Personal Data (PD)	PRI-05.5	Mechanisms exist to establish and maintain a current inventory of all Technology Assets, Applications and/or Services (TAAS) that collect, receive, process, store, transmit, share, update and/or dispose Personal	5	
PM-05(01)	Inventory of Personally Identifiable	Establish, maintain, and update [Assignment: organization-defined frequency] an inventory of all systems, applications, and projects that process personally identifiable information.	Functional	Intersects With	Personal Data (PD) Inventory Automation Support	PRI-05.6	Automated mechanisms exist to determine if Personal Data (PD) is maintained in electronic form.	5	
PM-06	Measures of Performance	Develop, monitor, and report on the results of information security and privacy measures of performance.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
PM-06	Measures of Performance	Develop, monitor, and report on the results of information security and privacy measures of performance.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
PM-07	Enterprise Architecture	Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5	
PM-08	Critical Infrastructure Plan	Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
PM-08	Critical Infrastructure Plan	Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
PM-09	Risk Management Strategy	Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information;b. Implement the risk management strategy consistently across the organization; andc. Review and update the risk management strategy [Assignment: organization-defined frequency] or as required, to address	Functional	Equal	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
PM-10	Authorization Process	a. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes;b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; andc. Integrate the authorization processes into an organization-wide risk management program.	Functional	Equal	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
PM-11	Mission and Business Process Definition	a. Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; andb. Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; andc. Review and revise the mission and business processes [Assignment: organization-defined frequency].	Functional	Equal	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	10	
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	
PM-13	Security and Privacy Workforce	Establish a security and privacy workforce development and improvement program.	Functional	Intersects With	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	
PM-14	Testing, Training, and Monitoring	a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems:1. Are developed and maintained; and2. Continue to be executed; andb. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	Functional	Intersects With	Personal Data (PD) Control Testing, Training & Monitoring	PRI-08	Mechanisms exist to conduct testing, training and monitoring activities for Personal Data (PD) controls.	5	
PM-14	Testing, Training, and Monitoring	a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems:1. Are developed and maintained; and2. Continue to be executed; andb. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
PM-15	Security and Privacy Groups and Associations	Establish and institutionalize contact with selected groups and associations within the security and privacy communities:a. To facilitate ongoing security and privacy education and training for organizational personnel;b. To maintain currency with recommended security and privacy practices, techniques, and technologies; andc. To share current security and privacy information, including threats, vulnerabilities, and incidents.	Functional	Intersects With	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
PM-15	Security and Privacy Groups and Associations	Establish and institutionalize contact with selected groups and associations within the security and privacy communities:a. To facilitate ongoing security and privacy education and training for organizational personnel;b. To maintain currency with recommended security and privacy practices, techniques, and technologies; andc. To share current security and privacy information, including threats, vulnerabilities, and incidents.	Functional	Intersects With	Contacts With Groups & Associations	GOV-07	Mechanisms exist to establish contact with selected groups and associations within the security, compliance and resilience communities to: (1) Facilitate ongoing cybersecurity and data protection education and training for organizational personnel; (2) Maintain currency with recommended cybersecurity and data protection practices, techniques and technologies; and (3) Share current cybersecurity and/or data protection-related information including threats, vulnerabilities and incidents.	5	
PM-17	Protecting Controlled Unclassified Information on External Systems	a. Establish policy and procedures to ensure that requirements for the protection of controlled unclassified information that is processed, stored or transmitted on external systems, are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards; andb. Review and update the policy and procedures [Assignment: organization-defined frequency].	Functional	Equal	Protecting Sensitive / Regulated Data on External Technology Assets, Applications and/or Services (TAAS)	DCH-13.3	Mechanisms exist to ensure that the requirements for the protection of sensitive/regulated data processed, stored or transmitted on external Technology Assets, Applications and/or Services (TAAS), are implemented in accordance with applicable statutory, regulatory	10	
PM-18	Privacy Program Plan	privacy program plan that provides an overview of the agency's privacy program, and:1. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program;2. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements;3. Includes the role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities;4. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program;5. Reflects coordination among organizational entities responsible for the different aspects of privacy; and6. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; andb. Update the plan [Assignment: organization-defined frequency] and to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or	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	
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	
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	(1) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role; (2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories; (3) Utilize publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy office(s) regarding data privacy practices; and (4) Inform data subjects when changes are made to the privacy notice and the nature of such	10	
PM-20(01)	Dissemination of Privacy Program Information | Privacy Policies on Websites, Applications, and Digital Services	Develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, that:a. Are written in plain language and organized in a way that is easy to understand and navigate;b. Provide information needed by the public to make an informed decision about whether and how to interact with the organization; andc. Are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.	Functional	Equal	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and	10	
PM-21	Accounting of Disclosures	a. Develop and maintain an accurate accounting of disclosures of personally identifiable information, including:1. Date, nature, and purpose of each disclosure; and2. Name and address, or other contact information of the individual or organization to which the disclosure was made;b. Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; andc. Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.	Functional	Equal	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by: (1) The organization; and/or (2) Relevant third-parties that their PD was shared with.	10	
PM-22	Personally Identifiable Information Quality Management	Develop and document organization-wide policies and procedures for:a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle;b. Correcting or deleting inaccurate or outdated personally identifiable information;c. Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities; andd. Appeals of adverse decisions on correction or deletion requests.	Functional	Intersects With	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
PM-22	Personally Identifiable Information Quality Management	Develop and document organization-wide policies and procedures for:a. Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle;b. Correcting or deleting inaccurate or outdated personally identifiable information;c. Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities; andd. Appeals of adverse decisions on correction or deletion requests.	Functional	Intersects With	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.	5	
PM-23	Data Governance Body	Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].	Functional	Intersects With	Data Management Board	PRI-13	Mechanisms exist to establish a written charter for a Data Management Board (DMB) and assigned organization-defined roles to the DMB.	5	
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	
PM-23	Data Governance Body	Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].	Functional	Intersects With	Data Governance	GOV-10	Mechanisms exist to facilitate data governance to oversee the organization's policies, standards and procedures so that sensitive/regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and contractual obligations.	5	
PM-24	Data Integrity Board	Establish a Data Integrity Board to:a. Review proposals to conduct or participate in a matching program; andb. Conduct an annual review of all matching programs in which the agency has participated.	Functional	Intersects With	Data Governance	GOV-10	Mechanisms exist to facilitate data governance to oversee the organization's policies, standards and procedures so that sensitive/regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and contractual obligations.	5	
PM-24	Data Integrity Board	Establish a Data Integrity Board to:a. Review proposals to conduct or participate in a matching program; andb. Conduct an annual review of all matching programs in which the agency has participated.	Functional	Intersects With	Data Management Board	PRI-13	Mechanisms exist to establish a written charter for a Data Management Board (DMB) and assigned organization-defined roles to the DMB.	5	
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	
PM-24	Data Integrity Board	Establish a Data Integrity Board to:a. Review proposals to conduct or participate in a matching program; andb. Conduct an annual review of all matching programs in which the agency has participated.	Functional	Intersects With	Personal Data (PD) Accuracy & Integrity	PRI-05.2	Mechanisms exist to ensure the accuracy and relevance of Personal Data (PD) throughout the information lifecycle by: (1) Keeping PD up-to-date; and	5	
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	
PM-24	Data Integrity Board	Establish a Data Integrity Board to:a. Review proposals to conduct or participate in a matching program; andb. Conduct an annual review of all matching programs in which the agency has participated.	Functional	Intersects With	Automated Data Management Processes	PRI-02.2	Automated mechanisms exist to adjust data that is able to be collected, received, processed, stored, transmitted, shared, updated and/or disposed, based on updated data subject authorization(s).	5	
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; andd. Review and update policies and procedures [Assignment: organization-defined frequency].	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and	5	
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	
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	
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; andd. Review and update policies and procedures [Assignment: organization-defined frequency].	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.	5	
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	
PM-26	Complaint Management	Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes:a. Mechanisms that are easy to use and readily accessible by the public;b. All information necessary for successfully filing complaints;c. Tracking mechanisms to ensure all complaints received are reviewed and addressed within [Assignment: organization-defined time period];d. Acknowledgement of receipt of complaints, concerns, or questions from individuals within [Assignment: organization-defined time period]; ande. Response to complaints, concerns, or questions from individuals within [Assignment: organization-defined time period].	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
PM-26	Complaint Management	Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes:a. Mechanisms that are easy to use and readily accessible by the public;b. All information necessary for successfully filing complaints;c. Tracking mechanisms to ensure all complaints received are reviewed and addressed within [Assignment: organization-defined time period];d. Acknowledgement of receipt of complaints, concerns, or questions from individuals within [Assignment: organization-defined time period]; ande. Response to complaints, concerns, or questions from individuals within [Assignment: organization-defined time period].	Functional	Intersects With	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.	5	
PM-27	Privacy Reporting	a. Develop [Assignment: organization-defined privacy reports] and disseminate to:1. [Assignment: organization-defined oversight bodies] to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and2. [Assignment: organization-defined officials] and other personnel with responsibility for monitoring privacy program compliance; andb. Review and update privacy reports [Assignment: organization-defined frequency].	Functional	Equal	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.	10	
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	
PM-29	Risk Management Program Leadership Roles	a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; andb. Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
PM-29	Risk Management Program Leadership Roles	a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; andb. Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
PM-29	Risk Management Program Leadership Roles	a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; andb. Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
PM-30(01)	Supply Chain Risk Management Strategy | Suppliers of Critical or Mission-essential Items	Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.	Functional	Intersects With	Customized Development of Critical Components	TDA-12	Mechanisms exist to custom-develop critical system components, when Commercial Off The Shelf (COTS) solutions are unavailable.	5	
PM-30(01)	Supply Chain Risk Management Strategy | Suppliers of Critical or Mission-essential Items	Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.	Functional	Intersects With	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	5	
PM-30(01)	Supply Chain Risk Management Strategy | Suppliers of Critical or Mission-essential Items	Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the	5	
PM-31	Continuous Monitoring Strategy	Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include:a. Establishing the following organization-wide metrics to be monitored: [Assignment: organization-defined metrics];b. Establishing [Assignment: organization-defined monitoring frequencies] and [Assignment: organization-defined assessment frequencies] for control effectiveness; c. Ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy;d. Correlation and analysis of information generated by control assessments and monitoring;e. Response actions to address results of the analysis of control assessment and monitoring information; andf. Reporting the security and privacy status of organizational systems to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
PS-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel security policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; andc. Review and update the current personnel security:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
PS-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel security policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; andc. Review and update the current personnel security:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
PS-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel security policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; andc. Review and update the current personnel security:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
PS-02	Position Risk Designation	a. Assign a risk designation to all organizational positions;b. Establish screening criteria for individuals filling those positions; andc. Review and update position risk designations [Assignment: organization-defined frequency].	Functional	Intersects With	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
PS-02	Position Risk Designation	a. Assign a risk designation to all organizational positions;b. Establish screening criteria for individuals filling those positions; andc. Review and update position risk designations [Assignment: organization-defined frequency].	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
PS-06	Access Agreements	a. Develop and document access agreements for organizational systems;b. Review and update the access agreements [Assignment: organization-defined frequency]; andc. Verify that individuals requiring access to organizational information and systems:1. Sign appropriate access agreements prior to being granted access; and2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [Assignment: organization-defined frequency].	Functional	Intersects With	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	5	
PS-06	Access Agreements	a. Develop and document access agreements for organizational systems;b. Review and update the access agreements [Assignment: organization-defined frequency]; andc. Verify that individuals requiring access to organizational information and systems:1. Sign appropriate access agreements prior to being granted access; and2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [Assignment: organization-defined frequency].	Functional	Intersects With	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	5	
PS-06(02)	Access Agreements | Classified Information Requiring Special Protection	Verify that access to classified information requiring special protection is granted only to individuals who:a. Have a valid access authorization that is demonstrated by assigned official government duties;b. Satisfy associated personnel security criteria; andc. Have read, understood, and signed a nondisclosure agreement.	Functional	Intersects With	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	5	
PS-06(02)	Access Agreements | Classified Information Requiring Special Protection	Verify that access to classified information requiring special protection is granted only to individuals who:a. Have a valid access authorization that is demonstrated by assigned official government duties;b. Satisfy associated personnel security criteria; andc. Have read, understood, and signed a nondisclosure	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	
PT-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personally identifiable information processing and transparency policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; andc. Review and update the current personally identifiable information processing and transparency:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
PT-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personally identifiable information processing and transparency policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; andc. Review and update the current personally identifiable information processing and transparency:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	

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

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

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
RA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; andc. Review and update the current risk assessment:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
RA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; andc. Review and update the current risk assessment:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
RA-03	Risk Assessment	a. Conduct a risk assessment, including:1. Identifying threats to and vulnerabilities in the system;2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;c. Document risk assessment results in [Selection (one): security and privacy plans; risk assessment report; [Assignment: organization-defined document]];d. Review risk assessment results [Assignment: organization-defined frequency];e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; andf. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	
RA-03	Risk Assessment	a. Conduct a risk assessment, including:1. Identifying threats to and vulnerabilities in the system;2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;c. Document risk assessment results in [Selection (one): security and privacy plans; risk assessment report; [Assignment: organization-defined document]];d. Review risk assessment results [Assignment: organization-defined frequency];e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; andf. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
RA-05	Vulnerability Monitoring and Scanning	and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:1. Enumerating platforms, software flaws, and improper configurations;2. Formatting checklists and test procedures; and3. Measuring vulnerability impact;c. Analyze vulnerability scan reports and results from vulnerability monitoring;d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk;e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; andf. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
RA-05	Vulnerability Monitoring and Scanning	and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:1. Enumerating platforms, software flaws, and improper configurations;2. Formatting checklists and test procedures; and3. Measuring vulnerability impact;c. Analyze vulnerability scan reports and results from vulnerability monitoring;d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk;e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; andf. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
RA-07	Risk Response	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.	Functional	Equal	Risk Response	RSK-06.1	proper risk response actions were performed to remediate findings from security, compliance and/or resilience-related: (1) Assessments;	10	
RA-08	Privacy Impact Assessments	Conduct privacy impact assessments for systems, programs, or other activities before:a. Developing or procuring information technology that processes personally identifiable information; andb. Initiating a new collection of personally identifiable information that:1. Will be processed using information technology; and2. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.	Functional	Equal	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
RA-09	Criticality Analysis	Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle].	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the	5	
RA-09	Criticality Analysis	Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle].	Functional	Intersects With	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	5	
RA-09	Criticality Analysis	Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle].	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle	5	
SA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; andc. Review and update the current system and services acquisition:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
SA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; andc. Review and update the current system and services acquisition:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
SA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; andc. Review and update the current system and services acquisition:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
SA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; andc. Review and update the current system and services acquisition:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
SA-02	Allocation of Resources	a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; andc. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.	Functional	Equal	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	10	
SA-03	System Development Life Cycle	a. Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations;b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;c. Identify individuals having information security and privacy roles and responsibilities; andd. Integrate the organizational information security and privacy risk management process into system development life cycle activities.	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5	
SA-03	System Development Life Cycle	a. Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations;b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;c. Identify individuals having information security and privacy roles and responsibilities; andd. Integrate the organizational information security and privacy risk management process into system development life cycle activities.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
SA-03(01)	System Development Life Cycle | Manage Preproduction Environment	Protect system preproduction environments commensurate with risk throughout the system development life cycle for the system, system component, or system service.	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5	
SA-03(01)	System Development Life Cycle | Manage Preproduction Environment	Protect system preproduction environments commensurate with risk throughout the system development life cycle for the system, system component, or system service.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
SA-03(01)	System Development Life Cycle | Manage Preproduction Environment	Protect system preproduction environments commensurate with risk throughout the system development life cycle for the system, system component, or system service.	Functional	Intersects With	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	5	
SA-03(03)	System Development Life Cycle | Technology Refresh	Plan for and implement a technology refresh schedule for the system throughout the system development life cycle.	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5	
SA-03(03)	System Development Life Cycle | Technology Refresh	Plan for and implement a technology refresh schedule for the system throughout the system development life cycle.	Functional	Intersects With	Refresh from Trusted Sources	SEA-08.1	Mechanisms exist to ensure that software and data needed for system component and service refreshes are obtained from trusted sources.	5	
SA-04	Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:a. Security and privacy functional requirements;b. Strength of mechanism requirements;c. Security and privacy assurance requirements;d. Controls needed to satisfy the security and privacy requirements.e. Security and privacy documentation requirements;f. Requirements for protecting security and privacy documentation;g. Description of the system development environment and environment in which the system is intended to operate;h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; andi. Acceptance criteria.	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5	
SA-04	Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:a. Security and privacy functional requirements;b. Strength of mechanism requirements;c. Security and privacy assurance requirements;d. Controls needed to satisfy the security and privacy requirements.e. Security and privacy documentation requirements;f. Requirements for protecting security and privacy documentation;g. Description of the system development environment and environment in which the system is intended to operate;h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; andi. Acceptance criteria.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
SA-04	Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:a. Security and privacy functional requirements;b. Strength of mechanism requirements;c. Security and privacy assurance requirements;d. Controls needed to satisfy the security and privacy requirements.e. Security and privacy documentation requirements;f. Requirements for protecting security and privacy documentation;g. Description of the system development environment and environment in which the system is intended to operate;h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; andi. Acceptance criteria.	Functional	Intersects With	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	5	
SA-04	Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:a. Security and privacy functional requirements;b. Strength of mechanism requirements;c. Security and privacy assurance requirements;d. Controls needed to satisfy the security and privacy requirements.e. Security and privacy documentation requirements;f. Requirements for protecting security and privacy documentation;g. Description of the system development environment and environment in which the system is intended to operate;h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; andi. Acceptance criteria.	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	5	
SA-04(01)	Acquisition Process | Functional Properties of Controls	Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.	Functional	Intersects With	Functional Properties	TDA-04.1	Mechanisms exist to require software developers to provide information describing the functional properties of the security, compliance and resilience controls to be utilized within Technology Assets, Applications and/or Services (TAAS) in sufficient detail to	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
SA-04(01)	Acquisition Process | Functional Properties of Controls	Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	5	
SA-04(02)	Acquisition Process | Design and Implementation Information for Controls	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of detail].	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	5	
SA-04(02)	Acquisition Process | Design and Implementation Information for Controls	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of detail].	Functional	Intersects With	Access to Program Source Code	TDA-20	Mechanisms exist to limit privileges to change software resident within software libraries.	5	
SA-04(02)	Acquisition Process | Design and Implementation Information for Controls	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of detail].	Functional	Intersects With	Functional Properties	TDA-04.1	Mechanisms exist to require software developers to provide information describing the functional properties of the security, compliance and resilience controls to be utilized within Technology Assets, Applications and/or Services (TAAS) in sufficient detail to	5	
SA-04(03)	Acquisition Process | Development Methods, Techniques, and Practices	Require the developer of the system, system component, or system service to demonstrate the use of a system development life cycle process that includes:a. [Assignment: organization-defined systems engineering methods];b. [Assignment: organization-defined [Selection (one or more): systems security; privacy] engineering methods]; andc. [Assignment: organization-defined software development methods; testing, evaluation, assessment, verification, and validation methods; and quality control processes].	Functional	Intersects With	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	5	
SA-04(03)	Acquisition Process | Development Methods, Techniques, and Practices	Require the developer of the system, system component, or system service to demonstrate the use of a system development life cycle process that includes:a. [Assignment: organization-defined systems engineering methods];b. [Assignment: organization-defined [Selection (one or more): systems security; privacy] engineering methods]; andc. [Assignment: organization-defined software development methods; testing, evaluation, assessment, verification, and validation methods; and quality control processes].	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
SA-04(12)	Acquisition Process | Data Ownership	a. Include organizational data ownership requirements in the acquisition contract; andb. Require all data to be removed from the contractor's system and returned to the organization within [Assignment: organization-defined time frame].	Functional	Intersects With	Personal Data (PD) Lineage	PRI-09	Mechanisms exist to maintain a process to document the lineage of Personal Data (PD) by recording how the organization collects, receives, processes, stores, transmits, shares,	5	
SA-04(12)	Acquisition Process | Data Ownership	a. Include organizational data ownership requirements in the acquisition contract; andb. Require all data to be removed from the contractor's system and returned to the organization within [Assignment: organization-defined time frame].	Functional	Intersects With	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	5	
SA-04(12)	Acquisition Process | Data Ownership	a. Include organizational data ownership requirements in the acquisition contract; andb. Require all data to be removed from the contractor's system and returned to the organization within [Assignment: organization-defined time frame].	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	5	
SA-05	System Documentation	a. Obtain or develop administrator documentation for the system, system component, or system service that describes:1. Secure configuration, installation, and operation of the system, component, or service;2. Effective use and maintenance of security and privacy functions and mechanisms; and3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;b. Obtain or develop user documentation for the system, system component, or system service that describes:1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [Assignment: organization-defined actions] in response; andd. Distribute documentation to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5	
SA-05	System Documentation	a. Obtain or develop administrator documentation for the system, system component, or system service that describes:1. Secure configuration, installation, and operation of the system, component, or service;2. Effective use and maintenance of security and privacy functions and mechanisms; and3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;b. Obtain or develop user documentation for the system, system component, or system service that describes:1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [Assignment: organization-defined actions] in response; andd. Distribute documentation to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).	5	
SA-08	Security and Privacy Engineering Principles	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
SA-08	Security and Privacy Engineering Principles	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or	5	
SA-08(30)	Security and Privacy Engineering Principles | Procedural Rigor	Implement the security design principle of procedural rigor in [Assignment: organization-defined systems or system components].	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
SA-08(30)	Security and Privacy Engineering Principles | Procedural Rigor	Implement the security design principle of procedural rigor in [Assignment: organization-defined systems or system components].	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5	
SA-08(31)	Security and Privacy Engineering Principles | Secure System Modification	Implement the security design principle of secure system modification in [Assignment: organization-defined systems or system components].	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
SA-08(31)	Security and Privacy Engineering Principles | Secure System Modification	Implement the security design principle of secure system modification in [Assignment: organization-defined systems or system components].	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	5	
SA-08(31)	Security and Privacy Engineering Principles | Secure System Modification	Implement the security design principle of secure system modification in [Assignment: organization-defined systems or system components].	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	5	
SA-08(33)	Security and Privacy Engineering Principles | Minimization	Implement the privacy principle of minimization using [Assignment: organization-defined processes].	Functional	Intersects With	Collection Minimization	END-13.3	Mechanisms exist to utilize sensors that are configured to minimize the collection of information about individuals.	5	
SA-08(33)	Security and Privacy Engineering Principles | Minimization	Implement the privacy principle of minimization using [Assignment: organization-defined processes].	Functional	Intersects With	Limit Sensitive / Regulated Data In Testing, Training & Research	DCH-18.2	Mechanisms exist to minimize the use of sensitive/regulated data for research, testing, or training, in accordance with authorized, legitimate business practices.	5	
SA-08(33)	Security and Privacy Engineering Principles | Minimization	Implement the privacy principle of minimization using [Assignment: organization-defined processes].	Functional	Intersects With	Minimize Visitor Personal Data (PD)	PES-06.5	Mechanisms exist to minimize the collection of Personal Data (PD) contained in visitor access records.	5	
SA-09	External System Services	a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls];b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; andc. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques].	Functional	Equal	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	10	
SA-09(05)	External System Services | Processing, Storage, and Service Location	Restrict the location of [Selection (one or more): information processing; information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	
SA-09(05)	External System Services | Processing, Storage, and Service Location	Restrict the location of [Selection (one or more): information processing; information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5	
SA-09(05)	External System Services | Processing, Storage, and Service Location	Restrict the location of [Selection (one or more): information processing; information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].	Functional	Intersects With	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.	5	
SA-09(08)	External System Services | Processing and Storage Location — U.S. Jurisdiction	Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States.	Functional	Intersects With	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.	5	
SA-09(08)	External System Services | Processing and Storage Location — U.S. Jurisdiction	Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	
SA-11	Developer Testing and Evaluation	Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:a. Develop and implement a plan for ongoing security and privacy control assessments;b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency] at [Assignment: organization-defined depth and coverage];c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;d. Implement a verifiable flaw remediation process; ande. Correct flaws identified during testing and evaluation.	Functional	Equal	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	10	
SA-11(02)	Developer Testing and Evaluation | Threat Modeling and Vulnerability Analyses	Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that:a. Uses the following contextual information: [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels];b. Employs the following tools and methods: [Assignment: organization-defined tools and methods];c. Conducts the modeling and analyses at the following level of rigor: [Assignment: organization-defined breadth and depth of modeling and analyses]; andd. Produces evidence that meets the following acceptance criteria: [Assignment: organization-defined acceptance criteria].	Functional	Intersects With	reat Analysis & Flaw	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Relationship	Notes
SA-11(02)	Developer Testing and Evaluation | Threat Modeling and Vulnerability Analyses	Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that:a. Uses the following contextual information: [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels];b. Employs the following tools and methods: [Assignment: organization-defined tools and methods];c. Conducts the modeling and analyses at the following level of rigor: [Assignment: organization-defined breadth and depth of modeling and analyses]; andd. Produces evidence that meets the following acceptance criteria: [Assignment: organization-defined acceptance criteria].	Functional	Intersects With	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	5	
SA-11(05)	Developer Testing and Evaluation | Penetration Testing	Require the developer of the system, system component, or system service to perform penetration testing:a. At the following level of rigor: [Assignment: organization-defined breadth and depth of testing]; andb. Under the following constraints: [Assignment: organization-defined constraints].	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	
SA-11(05)	Developer Testing and Evaluation | Penetration Testing	Require the developer of the system, system component, or system service to perform penetration testing:a. At the following level of rigor: [Assignment: organization-defined breadth and depth of testing]; andb. Under the following constraints: [Assignment: organization-defined constraints].	Functional	Intersects With	Application Penetration Testing	TDA-09.5	Mechanisms exist to perform application-level penetration testing of custom-made Technology Assets, Applications and/or Services (TAAS).	5	
SA-11(05)	Developer Testing and Evaluation | Penetration Testing	Require the developer of the system, system component, or system service to perform penetration testing:a. At the following level of rigor: [Assignment: organization-defined breadth and depth of testing]; andb. Under the following constraints: [Assignment: organization-defined constraints].	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	5	
SA-11(05)	Developer Testing and Evaluation | Penetration Testing	Require the developer of the system, system component, or system service to perform penetration testing:a. At the following level of rigor: [Assignment: organization-defined breadth and depth of testing]; andb. Under the following constraints: [Assignment: organization-defined constraints].	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; and/or (11) Artificial Intelligence and Autonomous Technologies (AAT).	5	
SA-11(05)	Developer Testing and Evaluation | Penetration Testing	Require the developer of the system, system component, or system service to perform penetration testing:a. At the following level of rigor: [Assignment: organization-defined breadth and depth of testing]; andb. Under the following constraints: [Assignment: organization-defined constraints].	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5	
SA-11(06)	Developer Testing and Evaluation | Attack Surface Reviews	Require the developer of the system, system component, or system service to perform attack surface reviews.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	5	
SA-11(06)	Developer Testing and Evaluation | Attack Surface Reviews	Require the developer of the system, system component, or system service to perform attack surface reviews.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	
SA-11(07)	Developer Testing and Evaluation | Verify Scope of Testing and Evaluation	Require the developer of the system, system component, or system service to verify that the scope of testing and evaluation provides complete coverage of the required controls at the following level of rigor: [Assignment: organization-defined breadth and depth of testing and evaluation].	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	
SA-11(07)	Developer Testing and Evaluation | Verify Scope of Testing and Evaluation	Require the developer of the system, system component, or system service to verify that the scope of testing and evaluation provides complete coverage of the required controls at the following level of rigor: [Assignment: organization-defined breadth and depth of testing and evaluation].	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	5	
SA-15(05)	Development Process, Standards, and Tools | Attack Surface Reduction	Require the developer of the system, system component, or system service to reduce attack surfaces to [Assignment: organization-defined thresholds].	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening	5	
SA-15(05)	Development Process, Standards, and Tools | Attack Surface Reduction	Require the developer of the system, system component, or system service to reduce attack surfaces to [Assignment: organization-defined thresholds].	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Relationship of	Notes
SA-22	Unsupported System Components	a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; orb. Provide the following options for alternative sources for continued support for unsupported components [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]].	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	TDA-17	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy	5	
SA-22	Unsupported System Components	a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; orb. Provide the following options for alternative sources for continued support for unsupported components [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]].	Functional	Intersects With	Alternate Sources for Continued Support	TDA-17.1	Mechanisms exist to provide in-house support or contract external providers for support with unsupported Technology Assets, Applications and/or Services (TAAS).	5	
SA-23	Specialization	Employ [Selection (one or more): design; modification; augmentation; reconfiguration] on [Assignment: organization-defined systems or system components] supporting mission essential services or functions to increase the trustworthiness in those systems or components.	Functional	Intersects With	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	5	
SA-23	Specialization	Employ [Selection (one or more): design; modification; augmentation; reconfiguration] on [Assignment: organization-defined systems or system components] supporting mission essential services or functions to increase the trustworthiness in those systems or components.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or	5	
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	
SC-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; andc. Review and update the current system and communications protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
SC-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; andc. Review and update the current system and communications protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
SC-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; andc. Review and update the current system and communications protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
SC-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; andc. Review and update the current system and communications protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
SC-03	Security Function Isolation	Isolate security functions from nonsecurity functions.	Functional	Intersects With	Restrict Access To Security Functions	END-16	Mechanisms exist to ensure security functions are restricted to authorized individuals and enforce least privilege control requirements for necessary job functions.	5	
SC-03	Security Function Isolation	Isolate security functions from nonsecurity functions.	Functional	Intersects With	Security Function Isolation	SEA-04.1	Mechanisms exist to isolate security functions from non-security functions.	5	
SC-05	Denial-of-service Protection	a. [Selection (one): Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]; andb. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event].	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5	
SC-05	Denial-of-service Protection	a. [Selection (one): Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]; andb. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event].	Functional	Intersects With	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	5	
SC-05	Denial-of-service Protection	a. [Selection (one): Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]; andb. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event].	Functional	Intersects With	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	5	
SC-05	Denial-of-service Protection	a. [Selection (one): Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]; andb. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event].	Functional	Intersects With	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	5	
SC-05(02)	Denial-of-service Protection | Capacity, Bandwidth, and Redundancy	Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks.	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5	
SC-05(02)	Denial-of-service Protection | Capacity, Bandwidth, and Redundancy	Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks.	Functional	Intersects With	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	5	
SC-07(08)	Boundary Protection | Route Traffic to Authenticated Proxy Servers	Route [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.	Functional	Intersects With	Route Internal Traffic to Proxy Servers	NET-18.1	Mechanisms exist to route internal communications traffic to external networks through organization-approved proxy servers at managed interfaces.	5	
SC-07(08)	Boundary Protection | Route Traffic to Authenticated Proxy Servers	Route [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
SC-07(09)	Boundary Protection | Restrict Threatening Outgoing Communications Traffic	a. Detect and deny outgoing communications traffic posing a threat to external systems; andb. Audit the identity of internal users associated with denied communications.	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
SC-07(09)	Boundary Protection | Restrict Threatening Outgoing Communications Traffic	a. Detect and deny outgoing communications traffic posing a threat to external systems; andb. Audit the identity of internal users associated with denied communications.	Functional	Intersects With	External Telecommunications Services	NET-03.2	Mechanisms exist to maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface.	5	
SC-07(10)	Boundary Protection | Prevent Exfiltration	a. Prevent the exfiltration of information; andb. Conduct exfiltration tests [Assignment: organization-defined frequency].	Functional	Intersects With	Prevent Unauthorized Exfiltration	NET-03.5	Automated mechanisms exist to prevent the unauthorized exfiltration of sensitive/regulated data across managed interfaces.	5	
SC-07(10)	Boundary Protection | Prevent Exfiltration	a. Prevent the exfiltration of information; andb. Conduct exfiltration tests [Assignment: organization-defined frequency].	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
SC-07(11)	Boundary Protection | Restrict Incoming Communications Traffic	Only allow incoming communications from [Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized destinations].	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	
SC-07(11)	Boundary Protection | Restrict Incoming Communications Traffic	Only allow incoming communications from [Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized destinations].	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
SC-07(14)	Boundary Protection | Protect Against Unauthorized Physical Connections	Protect against unauthorized physical connections at [Assignment: organization-defined managed interfaces].	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	
SC-07(14)	Protection | Protect Against Unauthorized Physical	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	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Relationship Strength of Relationsh	Notes
SC-07(14)	Boundary Protection | Protect Against Unauthorized Physical Connections	Protect against unauthorized physical connections at [Assignment: organization-defined managed interfaces].	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or	5	
SC-07(24)	Boundary Protection | Personally Identifiable Information	For systems that process personally identifiable information:a. Apply the following processing rules to data elements of personally identifiable information: [Assignment: organization-defined processing rules];b. Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system;c. Document each processing exception; andd. Review and remove exceptions that are no longer supported.	Functional	Equal	Personal Data (PD)	NET-03.4	Mechanisms exist to apply network-based processing rules to data elements of Personal Data (PD).	10	
SC-07(29)	Boundary Protection | Separate Subnets to Isolate Functions	Implement [Selection (one): physically; logically] separate subnetworks to isolate the following critical system components and functions: [Assignment: organization-defined critical system components and functions].	Functional	Intersects With	Cloud Infrastructure Security Subnet	CLD-03	Mechanisms exist to host security-specific technologies in a dedicated subnet.	5	
SC-07(29)	Boundary Protection | Separate Subnets to Isolate Functions	Implement [Selection (one): physically; logically] separate subnetworks to isolate the following critical system components and functions: [Assignment: organization-defined critical system components and functions].	Functional	Intersects With	Security Management Subnets	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the system.	5	
SC-07(29)	Boundary Protection | Separate Subnets to Isolate Functions	Implement [Selection (one): physically; logically] separate subnetworks to isolate the following critical system components and functions: [Assignment: organization-defined critical system components and functions].	Functional	Intersects With	Separate Subnet for Connecting to Different Security Domains	NET-03.8	Mechanisms exist to implement separate network addresses (e.g., different subnets) to connect to systems in different security domains.	5	
SC-08	Transmission Confidentiality and Integrity	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
SC-08	Transmission Confidentiality and Integrity	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
SC-08(01)	Transmission Confidentiality and Integrity | Cryptographic Protection	Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	Functional	Intersects With	Alternate Physical Protection	CRY-01.1	Cryptographic mechanisms exist to prevent unauthorized disclosure of information as an alternative to physical safeguards.	5	
SC-08(01)	Transmission Confidentiality and Integrity | Cryptographic Protection	Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
SC-08(01)	Transmission Confidentiality and Integrity | Cryptographic Protection	Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
SC-08(02)	Transmission Confidentiality and Integrity | Pre- and Post-transmission Handling	Maintain the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.	Functional	Intersects With	Pre/Post Transmission Handling	CRY-01.3	Cryptographic mechanisms exist to ensure the confidentiality and integrity of information during preparation for transmission and during reception.	5	
SC-08(02)	Transmission Confidentiality and Integrity | Pre- and Post-transmission Handling	Maintain the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
SC-08(02)	Transmission Confidentiality and Integrity | Pre- and Post-transmission Handling	Maintain the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.	Functional	Intersects With	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5	
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	
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	
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	
SC-16(01)	Transmission of Security and Privacy Attributes | Integrity Verification	Verify the integrity of transmitted security and privacy attributes.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
SC-16(01)	Transmission of Security and Privacy Attributes | Integrity Verification	Verify the integrity of transmitted security and privacy attributes.	Functional	Intersects With	Transmission of Cybersecurity & Data Protection Attributes	CRY-10	Mechanisms exist to associate Technology Assets, Applications and/or Services (TAAS) security attributes with information exchanged between TAAS.	5	
SC-18(01)	Mobile Code | Identify Unacceptable Code and Take Corrective Actions	Identify [Assignment: organization-defined unacceptable mobile code] and take [Assignment: organization-defined corrective actions].	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
SC-18(01)	Mobile Code | Identify Unacceptable Code and Take Corrective Actions	Identify [Assignment: organization-defined unacceptable mobile code] and take [Assignment: organization-defined corrective actions].	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
SC-18(01)	Mobile Code | Identify Unacceptable Code and Take Corrective Actions	Identify [Assignment: organization-defined unacceptable mobile code] and take [Assignment: organization-defined corrective actions].	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5	
SC-18(02)	Mobile Code | Acquisition, Development, and Use	Verify that the acquisition, development, and use of mobile code to be deployed in the system meets [Assignment: organization-defined mobile code requirements].	Functional	Intersects With	Software Licensing Restrictions	AST-02.7	Mechanisms exist to protect Intellectual Property (IP) rights with software licensing restrictions.	5	
SC-18(02)	Mobile Code | Acquisition, Development, and Use	Verify that the acquisition, development, and use of mobile code to be deployed in the system meets [Assignment: organization-defined mobile code requirements].	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
SC-18(03)	Mobile Code | Prevent Downloading and Execution	Prevent the download and execution of [Assignment: organization-defined unacceptable mobile code].	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
SC-18(03)	Mobile Code | Prevent Downloading and Execution	Prevent the download and execution of [Assignment: organization-defined unacceptable mobile code].	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
SC-18(04)	Mobile Code | Prevent Automatic Execution	Prevent the automatic execution of mobile code in [Assignment: organization-defined software applications] and enforce [Assignment: organization-defined actions] prior to executing the code.	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
SC-18(04)	Mobile Code | Prevent Automatic Execution	Prevent the automatic execution of mobile code in [Assignment: organization-defined software applications] and enforce [Assignment: organization-defined actions] prior to executing the code.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
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	
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	
SC-28(01)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5	
SC-28(01)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
SC-28(01)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
SC-28(01)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].	Functional	Intersects With	Encrypting Data In Storage Media	DCH-07.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	5	
SC-28(02)	Protection of Information at Rest | Offline Storage	Remove the following information from online storage and store offline in a secure location: [Assignment: organization-defined information].	Functional	Intersects With	Offline Storage	CRY-05.2	Mechanisms exist to remove unused data from online storage and archive it off-line in a secure location until it can be disposed of according to data retention requirements.	5	
SC-28(02)	Protection of Information at Rest | Offline Storage	Remove the following information from online storage and store offline in a secure location: [Assignment: organization-defined information].	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives	5	
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	
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	
SC-40	Wireless Link Protection	Protect external and internal [Assignment: organization-defined wireless links] from the following signal parameter attacks: [Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks].	Functional	Intersects With	Wireless Link Protection	NET-12.1	Mechanisms exist to protect external and internal wireless links from signal parameter attacks through monitoring for unauthorized wireless connections, including scanning for unauthorized wireless access points and taking appropriate action, if an unauthorized connection is discovered.	5	
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	
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	
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	
SI-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and information integrity policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; andc. Review and update the current system and information integrity:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
SI-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and information integrity policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; andc. Review and update the current system and information integrity:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
SI-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and information integrity policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; andc. Review and update the current system and information integrity:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
SI-02	Flaw Remediation	a. Identify, report, and correct system flaws;b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; andd. Incorporate flaw remediation into the organizational configuration management process.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
SI-02	Flaw Remediation	a. Identify, report, and correct system flaws;b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; andd. Incorporate flaw remediation into the organizational configuration management process.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
SI-02	Flaw Remediation	a. Identify, report, and correct system flaws;b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; andd. Incorporate flaw remediation into the organizational configuration management process.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5	
SI-02(04)	Flaw Remediation | Automated Patch Management Tools	Employ automated patch management tools to facilitate flaw remediation to the following system components: [Assignment: organization-defined system components].	Functional	Intersects With	Automated Remediation Status	VPM-05.2	Automated mechanisms exist to determine the state of system components with regard to flaw remediation.	5	
SI-02(04)	Flaw Remediation | Automated Patch Management Tools	Employ automated patch management tools to facilitate flaw remediation to the following system components: [Assignment: organization-defined system components].	Functional	Intersects With	Automated Software & Firmware Updates	VPM-05.4	Automated mechanisms exist to install the latest stable versions of security-relevant software and firmware updates.	5	
SI-02(04)	Flaw Remediation | Automated Patch Management Tools	Employ automated patch management tools to facilitate flaw remediation to the following system components: [Assignment: organization-defined system components].	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	
SI-02(04)	Flaw Remediation | Automated Patch Management Tools	Employ automated patch management tools to facilitate flaw remediation to the following system components: [Assignment: organization-defined system components].	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
SI-03	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;c. Configure malicious code protection mechanisms to:1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; andd. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
SI-03	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;c. Configure malicious code protection mechanisms to:1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; andd. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
SI-03	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;c. Configure malicious code protection mechanisms to:1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; andd. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
SI-03	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;c. Configure malicious code protection mechanisms to:1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; andd. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	Functional	Intersects With	Heuristic / Nonsignature-Based Detection	END-04.4	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5	
SI-03	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;c. Configure malicious code protection mechanisms to:1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; andd. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	
SI-03	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;c. Configure malicious code protection mechanisms to:1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; andd. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5	
SI-03	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;c. Configure malicious code protection mechanisms to:1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; andd. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
SI-04	System Monitoring	a. Monitor the system to detect:1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and2. Unauthorized local, network, and remote connections;b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];c. Invoke internal monitoring capabilities or deploy monitoring devices:1. Strategically within the system to collect organization-determined essential information; and2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;d. Analyze detected events and anomalies;e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;f. Obtain legal opinion regarding system monitoring activities; andg. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
SI-04	System Monitoring	a. Monitor the system to detect:1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and2. Unauthorized local, network, and remote connections;b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];c. Invoke internal monitoring capabilities or deploy monitoring devices:1. Strategically within the system to collect organization-determined essential information; and2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;d. Analyze detected events and anomalies;e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;f. Obtain legal opinion regarding system monitoring activities; andg. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
SI-04	System Monitoring	a. Monitor the system to detect:1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and2. Unauthorized local, network, and remote connections;b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];c. Invoke internal monitoring capabilities or deploy monitoring devices:1. Strategically within the system to collect organization-determined essential information; and2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;d. Analyze detected events and anomalies;e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;f. Obtain legal opinion regarding system monitoring activities; andg. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	
SI-04	System Monitoring	a. Monitor the system to detect:1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and2. Unauthorized local, network, and remote connections;b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];c. Invoke internal monitoring capabilities or deploy monitoring devices:1. Strategically within the system to collect organization-determined essential information; and2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;d. Analyze detected events and anomalies;e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;f. Obtain legal opinion regarding system monitoring activities; andg. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
SI-04(07)	System Monitoring | Automated Response to Suspicious Events	a. Notify [Assignment: organization-defined incident response personnel (identified by name and/or by role)] of detected suspicious events; andb. Take the following actions upon detection: [Assignment: organization-defined least-disruptive actions to terminate suspicious events].	Functional	Intersects With	Automated Response to Suspicious Events	MON-01.11	Automated mechanisms exist to implement pre-determined corrective actions in response to detected events that have security incident implications.	5	
SI-04(07)	System Monitoring | Automated Response to Suspicious Events	a. Notify [Assignment: organization-defined incident response personnel (identified by name and/or by role)] of detected suspicious events; andb. Take the following actions upon detection: [Assignment: organization-defined least-disruptive actions to terminate suspicious events].	Functional	Intersects With	Automated Incident Handling Processes	IRO-02.1	Automated mechanisms exist to support the incident handling process.	5	
SI-04(12)	System Monitoring | Automated Organization-generated Alerts	Alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [Assignment: organization-defined activities that trigger alerts].	Functional	Intersects With	Automated Alerts	MON-01.12	Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.	5	
SI-04(12)	System Monitoring | Automated Organization-generated Alerts	Alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [Assignment: organization-defined activities that trigger alerts].	Functional	Intersects With	Real-Time Alerts of Event Logging Failure	MON-05.1	Mechanisms exist to provide 24x7x365 near real-time alerting capability when an event log processing failure occurs.	5	
SI-04(18)	System Monitoring | Analyze Traffic and Covert Exfiltration	Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information: [Assignment: organization-defined interior points within the system].	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
SI-04(18)	System Monitoring | Analyze Traffic and Covert Exfiltration	Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information: [Assignment: organization-defined interior points within the system].	Functional	Intersects With	Analyze Traffic for Covert Exfiltration	MON-11.1	Automated mechanisms exist to analyze network traffic to detect covert data exfiltration.	5	
SI-04(24)	System Monitoring | Indicators of Compromise	Discover, collect, and distribute to [Assignment: organization-defined personnel or roles], indicators of compromise provided by [Assignment: organization-defined sources].	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	5	
SI-04(24)	System Monitoring | Indicators of Compromise	Discover, collect, and distribute to [Assignment: organization-defined personnel or roles], indicators of compromise provided by [Assignment: organization-defined sources].	Functional	Intersects With	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets, Applications and/or Services (TAAS) to generate alerts for unauthorized modifications.	5	
SI-04(25)	System Monitoring | Optimize Network Traffic Analysis	Provide visibility into network traffic at external and key internal system interfaces to optimize the effectiveness of monitoring devices.	Functional	Intersects With	Limit Network Connections	NET-03.1	Mechanisms exist to limit the number of concurrent external network connections to its Technology Assets, Applications and/or Services (TAAS).	5	
SI-04(25)	System Monitoring | Optimize Network Traffic Analysis	Provide visibility into network traffic at external and key internal system interfaces to optimize the effectiveness of monitoring devices.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
SI-05	Security Alerts, Advisories, and Directives	a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;b. Generate internal security alerts, advisories, and directives as deemed necessary;c. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; andd. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
SI-05	Security Alerts, Advisories, and Directives	a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;b. Generate internal security alerts, advisories, and directives as deemed necessary;c. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; andd. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
SI-05	Security Alerts, Advisories, and Directives	a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;b. Generate internal security alerts, advisories, and directives as deemed necessary;c. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; andd. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	
SI-07	Software, Firmware, and Information Integrity	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; andb. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	5	
SI-07	Software, Firmware, and Information Integrity	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; andb. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	
SI-07	Software, Firmware, and Information Integrity	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; andb. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
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	
SI-10	Information Input Validation	Check the validity of the following information inputs: [Assignment: organization-defined information inputs to the system]	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
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	
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	
SI-12(01)	Information Management and Retention | Limit Personally Identifiable Information Elements	Limit personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: [Assignment: organization-defined elements of personally identifiable information].	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.	5	
SI-12(01)	Information Management and Retention | Limit Personally Identifiable Information Elements	Limit personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: [Assignment: organization-defined elements of personally identifiable information].	Functional	Intersects With	Minimize Sensitive / Regulated Data	DCH-18.1	Mechanisms exist to minimize sensitive/regulated data that is collected, received, processed, stored and/or transmitted throughout the information lifecycle to only those elements necessary to support necessary	5	
SI-12(02)	Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training, and Research	Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: [Assignment: organization-defined techniques].	Functional	Intersects With	Limit Sensitive / Regulated Data In Testing, Training & Research	DCH-18.2	Mechanisms exist to minimize the use of sensitive/regulated data for research, testing, or training, in accordance with authorized, legitimate business practices.	5	
SI-12(02)	Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training, and Research	Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: [Assignment: organization-defined techniques].	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.	5	
SI-12(03)	Information Management and Retention | Information Disposal	Use the following techniques to dispose of, destroy, or erase information following the retention period: [Assignment: organization-defined techniques].	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	
SI-12(03)	Information Management and Retention | Information Disposal	Use the following techniques to dispose of, destroy, or erase information following the retention period: [Assignment: organization-defined techniques].	Functional	Intersects With	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	5	
SI-13	Predictable Failure Prevention	a. Determine mean time to failure (MTTF) for the following system components in specific environments of operation: [Assignment: organization-defined system components]; andb. Provide substitute system components and a means to exchange active and standby components in accordance with the following criteria: [Assignment: organization-defined MTTF substitution criteria]	Functional	Intersects With	Failover Capability	BCD-12.2	Mechanisms exist to implement real-time or near-real-time failover capability to maintain availability of critical Technology Assets, Applications, Services and/or Data (TAASD).	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
SI-13	Predictable Failure Prevention	a. Determine mean time to failure (MTTF) for the following system components in specific environments of operation: [Assignment: organization-defined system components]; andb. Provide substitute system components and a means to exchange active and standby components in accordance with the following criteria: [Assignment: organization-defined MTTF substitution criteria]	Functional	Intersects With	Predictable Failure Analysis	SEA-07	Mechanisms exist to determine the Mean Time to Failure (MTTF) for system components in specific environments of operation.	5	
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	
SI-18(04)	Personally Identifiable Information Quality Operations | Individual Requests	Correct or delete personally identifiable information upon request by individuals or their designated representatives.	Functional	Intersects With	Correcting Inaccurate Personal Data (PD)	PRI-06.1	Mechanisms exist to maintain a process for: (1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and (2) Disseminating corrections or amendments of PD to other authorized users of the PD.	5	
SI-18(04)	Personally Identifiable Information Quality Operations | Individual Requests	Correct or delete personally identifiable information upon request by individuals or their designated representatives.	Functional	Intersects With	Updating & Correcting Personal Data (PD)	DCH-22.1	Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.	5	
SI-18(04)	Personally Identifiable Information Quality Operations | Individual Requests	Correct or delete personally identifiable information upon request by individuals or their designated representatives.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
SI-18(05)	Personally Identifiable Information Quality Operations | Notice of Correction or Deletion	Notify [Assignment: organization-defined recipients of personally identifiable information] and individuals that the personally identifiable information has been corrected or deleted.	Functional	Intersects With	Updating & Correcting Personal Data (PD)	DCH-22.1	Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.	5	
SI-18(05)	Personally Identifiable Information Quality Operations | Notice of Correction or Deletion	Notify [Assignment: organization-defined recipients of personally identifiable information] and individuals that the personally identifiable information has been corrected or deleted.	Functional	Intersects With	Correcting Inaccurate Personal Data (PD)	PRI-06.1	Mechanisms exist to maintain a process for: (1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and (2) Disseminating corrections or amendments of PD to other authorized users of the PD.	5	
SI-18(05)	Personally Identifiable Information Quality Operations | Notice of Correction or	Notify [Assignment: organization-defined recipients of personally identifiable information] and individuals that the personally identifiable information has been corrected or deleted.	Functional	Intersects With	Notice of Correction or Processing Change	PRI-06.2	Mechanisms exist to notify affected data subjects if their Personal Data (PD) has been corrected, amended or deleted.	5	
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	
SI-19(01)	De-identification | Collection	De-identify the dataset upon collection by not collecting personally identifiable information.	Functional	Intersects With	Primary Source Personal Data (PD) Collection	DCH-22.3	Mechanisms exist to collect Personal Data (PD) directly from the individual.	5	
SI-19(01)	De-identification | Collection	De-identify the dataset upon collection by not collecting personally identifiable information.	Functional	Intersects With	De-Identify Dataset Upon Collection	DCH-23.1	Mechanisms exist to de-identify the dataset upon collection by not collecting Personal Data (PD).	5	
SI-19(04)	De-identification | Removal, Masking, Encryption, Hashing, or Replacement of Direct Identifiers	Remove, mask, encrypt, hash, or replace direct identifiers in a dataset.	Functional	Intersects With	Data Masking	PRI-05.3	Mechanisms exist to mask sensitive/regulated data through data anonymization, pseudonymization, redaction or de-identification.	5	
SI-19(04)	De-identification | Removal, Masking, Encryption, Hashing, or Replacement of Direct Identifiers	Remove, mask, encrypt, hash, or replace direct identifiers in a dataset.	Functional	Intersects With	Removal, Masking, Encryption, Hashing or Replacement of Direct Identifiers	DCH-23.4	Mechanisms exist to remove, mask, encrypt, hash or replace direct identifiers in a dataset.	5	
SR-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] supply chain risk management policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; andc. Review and update the current supply chain risk management:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
SR-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] supply chain risk management policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; andc. Review and update the current supply chain risk management:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
SR-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] supply chain risk management policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; andc. Review and update the current supply chain risk management:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
SR-02	Supply Chain Risk Management Plan	a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: [Assignment: organization-defined systems, system components, or system services];b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency] or as required, to address threat, organizational or environmental changes; andc. Protect the supply chain risk management plan from unauthorized disclosure and modification.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
SR-02	Supply Chain Risk Management Plan	a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: [Assignment: organization-defined systems, system components, or system services];b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency] or as required, to address threat, organizational or environmental changes; andc. Protect the supply chain risk management plan from unauthorized disclosure and modification.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
SR-03(01)	Supply Chain Controls and Processes | Diverse Supply Base	Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].	Functional	Intersects With	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	5	
SR-03(01)	Supply Chain Controls and Processes | Diverse Supply Base	Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].	Functional	Intersects With	Supplier Diversity	TDA-03.1	Mechanisms exist to obtain security, compliance and resilience technologies from different suppliers to minimize supply chain risk.	5	
SR-03(01)	Supply Chain Controls and Processes | Diverse Supply Base	Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services.	5	
SR-03(03)	Supply Chain Controls and Processes | Sub-tier Flow Down	Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5	
SR-03(03)	Supply Chain Controls and Processes | Sub-tier Flow Down	Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
SR-07	Supply Chain Operations Security	Employ the following Operations Security (OPSEC) controls to protect supply chain-related information for the system, system component, or system service: [Assignment: organization-defined Operations Security (OPSEC) controls].	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
SR-07	Supply Chain Operations Security	Employ the following Operations Security (OPSEC) controls to protect supply chain-related information for the system, system component, or system service: [Assignment: organization-defined Operations Security (OPSEC) controls].	Functional	Intersects With	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	5	
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	
SR-10	Inspection of Systems or Components	Inspect the following systems or system components [Selection (one or more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering: [Assignment: organization-defined systems or system components].	Functional	Intersects With	Technology Asset Inspections	AST-15.1	Mechanisms exist to physically and logically inspect critical technology assets to detect evidence of tampering.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh	Notes
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	