

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference document: Secure Controls Framework (SCF) version 2026.1

STRM Guidance: <https://securecontrolsframework.com/set-theory-relationship-mapping-strm/>**Focal Document: NIST SP 800-160 Volume 2, Revision 1**Focal Document URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf>Published STRM URL: <https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-160-vol-2-r1.pdf>

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	of Relationships	Notes
AC-02(06)	Account Management Dynamic Privilege Management	Implement [Assignment: organization-defined dynamic privilege management capabilities].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
AC-02(08)	Account Management Dynamic Account Management	Create, activate, manage, and deactivate [Assignment: organization-defined system accounts] dynamically.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
AC-02(12)	Account Management Account Monitoring for Atypical Usage	a. Monitor system accounts for [Assignment: organization-defined atypical usage]; andb. Report atypical usage of system accounts to [Assignment: organization-defined personnel or roles].	Functional	Equal	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	10	
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(07)	Access Enforcement Role-based Access Control	Enforce a role-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined roles and users authorized to assume such roles].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
AC-03(11)	Access Enforcement Restrict Access to Specific Information Types	Restrict access to data repositories containing [Assignment: organization-defined information types].	Functional	Equal	Sensitive / Regulated Data Access Enforcement	CFG-08	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to restrict access to sensitive/regulated data.	10	
AC-03(12)	Access Enforcement Assert and Enforce Application Access	a. Require applications to assert, as part of the installation process, the access needed to the following system applications and functions: [Assignment: organization-defined system applications and functions];b. Provide an enforcement mechanism to prevent unauthorized access; andc. Approve access changes after initial installation of the application.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
AC-03(13)	Access Enforcement Attribute-based Access Control	Enforce attribute-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined attributes to assume access decisions].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
AC-04(02)	Information Flow Enforcement Processing Domains	Use protected processing domains to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
AC-04(03)	Information Flow Enforcement Dynamic Information Flow Control	Enforce [Assignment: organization-defined information flow control policies].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
AC-04(08)	Information Flow Enforcement Security and Privacy Policy Filters	a. Enforce information flow control using [Assignment: organization-defined security or privacy policy filters] as a basis for flow control decisions for [Assignment: organization-defined information flows]; andb. [Selection (one or more): Block; Strip; Modify; Quarantine] data after a filter processing failure in accordance with [Assignment: organization-defined security or privacy policy].	Functional	Equal	Policy Decision Point (PDP)	NET-04.7	Automated mechanisms exist to evaluate access requests against established criteria to dynamically and uniformly enforce access rights and permissions.	10	
AC-04(12)	Information Flow Enforcement Data Type Identifiers	When transferring information between different security domains, use [Assignment: organization-defined data type identifiers] to validate data essential for information flow decisions.	Functional	Equal	Data Type Identifiers	NET-04.8	Automated mechanisms exist to utilize data type identifiers to validate data essential for information flow decisions when transferring information between different security domains.	10	
AC-04(17)	Information Flow Enforcement Domain Authentication	Uniquely identify and authenticate source and destination points by [Selection (one or more): organization; system; application; service; individual] for information transfer.	Functional	Equal	Cross Domain Authentication	NET-04.12	Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.	10	
AC-04(21)	Information Flow Enforcement Physical or Logical Separation of Information Flows	Separate information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization-defined required separations by types of information].	Functional	Equal	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	10	
AC-04(27)	Information Flow Enforcement Redundant/independent Filtering Mechanisms	When transferring information between different security domains, implement content filtering solutions that provide redundant and independent filtering mechanisms for each data type.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
AC-04(29)	Information Flow Enforcement Filter Orchestration Engines	When transferring information between different security domains, employ content filter orchestration engines to ensure that:a. Content filtering mechanisms successfully complete execution without errors; andb. Content filtering actions occur in the correct order and comply with [Assignment: organization-defined policy].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
AC-04(30)	Information Flow Enforcement Filter Mechanisms Using Multiple Processes	When transferring information between different security domains, implement content filtering mechanisms using multiple processes.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
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-06(01)	Least Privilege Authorize Access to Security Functions	Authorize access for [Assignment: organization-defined individuals or roles] to:a. [Assignment: organization-defined security functions] (deployed in hardware, software, and firmware); andb. [Assignment: organization-defined security-relevant information].	Functional	Equal	Authorize Access to Security Functions	IAC-21.1	Mechanisms exist to limit access to security functions to explicitly-authorized privileged users.	10	
AC-06(02)	Least Privilege Non-privileged Access for Nonsecurity Functions	Require that users of system accounts (or roles) with access to [Assignment: organization-defined security functions or security-relevant information] use non-privileged accounts or roles, when accessing nonsecurity functions.	Functional	Equal	Non-Privileged Access for Non-Security Functions	IAC-21.2	Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.	10	
AC-06(03)	Least Privilege Network Access to Privileged Commands	Authorize network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and document the rationale for such access in the security plan for the system.	Functional	Equal	Network Access to Privileged Commands	IAC-21.6	Mechanisms exist to authorize remote access to perform privileged commands on critical Technology Assets, Applications and/or Services (TAAS) or where sensitive/regulated data is stored, transmitted and/or processed only for compelling operational needs.	10	
AC-06(04)	Least Privilege Separate Processing Domains	Provide separate processing domains to enable finer-grained allocation of user privileges.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
AC-06(05)	Least Privilege Privileged Accounts	Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].	Functional	Equal	Management Approval For Privileged Accounts	IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	of Relationships	Notes
AC-06(06)	Least Privilege Privileged Access by Non-organizational Users	Prohibit privileged access to the system by non-organizational users.	Functional	Equal	Privileged Access by Non-Organizational Users	IAC-05.2	Mechanisms exist to prohibit privileged access by non-organizational users.	10	
AC-06(07)	Least Privilege Review of User Privileges	a. Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; andb. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.	Functional	Equal	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	10	
AC-06(08)	Least Privilege Privilege Levels for Code Execution	Prevent the following software from executing at higher privilege levels than users executing the software: [Assignment: organization-defined software].	Functional	Equal	Privilege Levels for Code Execution	IAC-21.7	Automated mechanisms exist to prevent applications from executing at higher privilege levels than the user's privileges.	10	
AC-06(10)	Least Privilege Prohibit Non-privileged Users from Executing Privileged Functions	Prevent non-privileged users from executing privileged functions.	Functional	Equal	Prohibit Non-Privileged Users from Executing Privileged Functions	IAC-21.5	Mechanisms exist to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures.	10	
AC-07(04)	Unsuccessful Logon Attempts Use of Alternate Authentication Factor	a. Allow the use of [Assignment: organization-defined authentication factors] that are different from the primary authentication factors after the number of organization-defined consecutive invalid logon attempts have been exceeded; andb. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts through use of the alternative factors by a user during a [Assignment: organization-defined time period].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
AC-12	Session Termination	Automatically terminate a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].	Functional	Equal	Session Termination	IAC-25	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.	10	
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: <u>The purpose(s) originally</u>	5	
AT-02(01)	Literacy Training and Awareness Practical Exercises	Provide practical exercises in literacy training that simulate events and incidents.	Functional	Intersects With	Simulated Cyber Attack Scenario Training	SAT-02.1	Mechanisms exist to include simulated actual cyber-attacks through practical exercises that are aligned with current threat scenarios.	5	
AT-02(03)	Literacy Training and Awareness Social Engineering and Mining	Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.	Functional	Equal	Social Engineering & Mining	SAT-02.2	Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social	10	
AT-02(05)	Literacy Training and Awareness Advanced Persistent Threat	Provide literacy training on the advanced persistent threat.	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5	
AT-03(03)	Role-based Training Practical Exercises	Provide practical exercises in security and privacy training that reinforce training objectives.	Functional	Equal	Practical Exercises	SAT-03.1	Mechanisms exist to include practical exercises in security, compliance and resilience training that reinforce training objectives.	10	
AU-05(03)	Response to Audit Logging Process Failures Configurable Traffic Volume Thresholds	Enforce configurable network communications traffic volume thresholds reflecting limits on audit log storage capacity and [Selection: reject; delay] network traffic above those thresholds.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
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-06(03)	Audit Record Review, Analysis, and Reporting Correlate Audit Record Repositories	Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
AU-06(05)	Audit Record Review, Analysis, and Reporting Integrated Analysis of Audit Records	Integrate analysis of audit records with analysis of [Selection (one or more): vulnerability scanning information; performance data; system monitoring information; [Assignment: organization-defined data/information collected from other sources]] to further enhance the ability to identify inappropriate or unusual activity.	Functional	Equal	Integration of Scanning & Other Monitoring Information	MON-02.3	Automated mechanisms exist to integrate the analysis of audit records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further enhance the ability to identify inappropriate or unusual activity.	10	
AU-06(06)	Audit Record Review, Analysis, and Reporting Correlation with Physical Monitoring	Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.	Functional	Equal	Correlation with Physical Monitoring	MON-02.4	Automated mechanisms exist to correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual or malevolent activity.	10	
AU-06(08)	Review, Analysis, and Reporting Full Text Analysis of Privileged	Perform a full text analysis of logged privileged commands in a physically distinct component or subsystem of the system, or other system that is dedicated to that analysis.	Functional	Equal	Privileged Functions Logging	MON-03.3	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	10	
AU-06(09)	Audit Record Review, Analysis, and Reporting Correlation with Information from Nontechnical Sources	Correlate information from nontechnical sources with audit record information to enhance organization-wide situational awareness.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	of Relationships	Notes
AU-09(01)	Protection of Audit Information Hardware Write-once Media	Write audit trails to hardware-enforced, write-once media.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
AU-09(02)	Protection of Audit Information Store on Separate Physical Systems or Components	Store audit records [Assignment: organization-defined frequency] in a repository that is part of a physically different system or system component than the system or component being audited.	Functional	Intersects With	Event Log Backup on Separate Physical Systems / Components	MON-08.1	Mechanisms exist to back up event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or similar automated tool.	5	
AU-09(03)	Protection of Audit Information Cryptographic Protection	Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.	Functional	Equal	Cryptographic Protection of Event Log Information	MON-08.3	Cryptographic mechanisms exist to protect the integrity of event logs and audit tools.	10	
AU-09(05)	Protection of Audit Information Dual Authorization	Enforce dual authorization for [Selection (one or more): movement; deletion] of [Assignment: organization-defined audit information].	Functional	Equal	Dual Authorization for Event Log Movement	MON-08.4	Automated mechanisms exist to enforce dual authorization for the movement or deletion of event logs.	10	
AU-09(06)	Protection of Audit Information Read-only Access	Authorize read-only access to audit information to [Assignment: organization-defined subset of privileged users or roles].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
AU-09(07)	Protection of Audit Information Store on Component with Different Operating System	Store audit information on a component running a different operating system than the system or component being audited.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
AU-10(02)	Non-repudiation Validate Binding of Information Producer Identity	a. Validate the binding of the information producer identity to the information at [Assignment: organization-defined frequency]; andb. Perform [Assignment: organization-defined actions] in the event of [Assignment: organization-defined open-source information and/or information sites]	Functional	Intersects With	Identity Binding	MON-09.1	Mechanisms exist to bind the identity of the information producer to the information generated.	5	
AU-13	Monitoring for Information Disclosure	[Assignment: organization-defined frequency] for evidence of unauthorized disclosure of organizational information; andb. If an information disclosure is discovered:1. Notify [Assignment: organization-defined personnel or roles]; and2. Take the following additional actions: [Assignment: organization-defined additional actions]	Functional	Equal	Monitoring For Information Disclosure	MON-11	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of non-public information.	10	
AU-13(03)	Monitoring for Information Disclosure Unauthorized Replication of Information	Employ discovery techniques, processes, and tools to determine if external entities are replicating organizational information in an unauthorized manner.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CA-07(03)	Continuous Monitoring Trend Analyses	Employ trend analyses to determine if control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data.	Functional	Equal	Trend Analysis Reporting	MON-06.2	Mechanisms exist to employ trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.	10	
CA-07(05)	Continuous Monitoring Consistency Analysis	Employ the following actions to validate that policies are established and implemented controls are operating in a consistent manner: [Assignment: organization-defined actions]	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CA-07(06)	Continuous Monitoring Automation Support for Monitoring	Ensure the accuracy, currency, and availability of monitoring results for the system using [Assignment: organization-defined automated mechanisms].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CA-08	Penetration Testing	Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components].	Functional	Equal	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	10	
CA-08(01)	Penetration Testing Independent Penetration Testing Agent or Team	Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.	Functional	Equal	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	10	
CA-08(02)	Penetration Testing Red Team Exercises	Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement: [Assignment: organization-defined red team exercises].	Functional	Equal	Red Team Exercises	VPM-10	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise Technology Assets, Applications and/or Services (TAAS) in accordance with organization-defined rules of	10	
CA-08(03)	Penetration Testing Facility Penetration Testing	Employ a penetration testing process that includes [Assignment: organization-defined frequency] [Selection (one or more): announced; unannounced] attempts to bypass or circumvent controls associated with physical access points to the facility.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CM-02(07)	Baseline Configuration Configure Systems and Components for High-risk Areas	a. Issue [Assignment: organization-defined systems or system components] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; andb. Apply the following controls to the systems or components when the individuals return from travel: [Assignment: organization-defined controls].	Functional	Equal	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	10	
CM-04(01)	Impact Analyses Separate Test Environments	Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.	Functional	Equal	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS).	10	
CM-05(04)	Access Restrictions for Change Dual Authorization	Enforce dual authorization for implementing changes to [Assignment: organization-defined system components and system-level information].	Functional	Equal	Dual Authorization for Change	CHG-04.3	Mechanisms exist to enforce a two-person rule for implementing changes to critical Technology Assets, Applications and/or Services (TAAS).	10	
CM-05(05)	Access Restrictions for Change Privilege Limitation for Production and Operation	a. Limit privileges to change system components and system-related information within a production or operational environment; andb. Review and reevaluate privileges [Assignment: organization-defined frequency].	Functional	Equal	Permissions To Implement Changes	CHG-04.4	Mechanisms exist to limit operational privileges for implementing changes.	10	
CM-05(06)	Access Restrictions for Change Limit Library Privileges	Limit privileges to change software resident within software libraries.	Functional	Equal	Library Privileges	CHG-04.5	Mechanisms exist to restrict software library privileges to those individuals with a pertinent business need for access.	10	
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-07(04)	Least Functionality Unauthorized Software — Deny-by-exception	a. Identify [Assignment: organization-defined software programs not authorized to execute on the system];b. Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; andc. Review and update the list of unauthorized software programs [Assignment: organization-defined frequency].	Functional	Equal	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	of Relationships	Notes
CM-07(05)	Least Functionality Authorized Software — Allow-by-exception	a. Identify [Assignment: organization-defined software programs authorized to execute on the system]; b. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and c. Review and update the list of authorized software programs [Assignment: organization-defined frequency].	Functional	Equal	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	10	
CM-07(06)	Least Functionality Confined Environments with Limited Privileges	Require that the following user-installed software execute in a confined physical or virtual machine environment with limited privileges: [Assignment: organization-defined user-installed software].	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	
CM-07(07)	Least Functionality Code Execution in Protected Environments	Prevent execution of binary or machine-executable code only in confined physical or virtual machine environments and with the explicit approval of [Assignment: organization-defined personnel or roles] when such code is a. Obtained from sources with limited or no warranty; and/or b. Without the provision of [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	
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]; and b. Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].	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]; and b. Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].	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]; and b. Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].	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-14	Signed Components	Prevent the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.	Functional	Intersects With	Signed Components	CHG-04.2	Mechanisms exist to prevent the installation of software and firmware components without verification that the component has been digitally signed using an organization-approved certificate authority.	5	
CP-02(01)	Contingency Plan Coordinate with Related Plans	Coordinate contingency plan development with organizational elements responsible for related plans.	Functional	Equal	Coordinate with Related Plans	BCD-01.1	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	10	
CP-02(05)	Contingency Plan Continue Mission and Business Functions	Plan for the continuance of [Selection (one): all; essential] mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.	Functional	Equal	Continue Essential Mission & Business Functions	BCD-02.2	Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration at primary processing and/or storage sites.	10	
CP-02(08)	Contingency Plan Identify Critical Assets	Identify critical system assets supporting [Selection (one): all; essential] mission and business functions.	Functional	Equal	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	10	
CP-04(05)	Contingency Plan Testing Self-challenge	Employ [Assignment: organization-defined mechanisms] to [Assignment: organization-defined system or system component] to disrupt and adversely affect the system or system component.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CP-08(03)	Telecommunications Services Separation of Primary and Alternate Providers	Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.	Functional	Equal	Separation of Primary / Alternate Providers	BCD-10.2	Mechanisms exist to obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.	10	
CP-09	System Backup	a. Conduct backups of user-level information contained in [Assignment: organization-defined system components] [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; c. Conduct backups of system documentation, including security- and privacy-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and d. Protect the confidentiality, integrity, and availability of backup information.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
CP-09(01)	System Backup Testing for Reliability and Integrity	Test backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.	Functional	Equal	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	10	
CP-09(06)	System Backup Redundant Secondary System	Conduct system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations.	Functional	Equal	Redundant Secondary System	BCD-11.7	Mechanisms exist to maintain a failover capability, which is not collocated with the primary Technology Asset, Application and/or Service (TAAS), which can be activated with little-to-no loss of information or disruption to operations.	10	
CP-09(07)	System Backup Dual Authorization for Deletion or Destruction	Enforce dual authorization for the deletion or destruction of [Assignment: organization-defined backup information].	Functional	Equal	Dual Authorization For Backup Media Destruction	BCD-11.8	Mechanisms exist to implement and enforce dual authorization for the deletion or destruction of sensitive backup media and data.	10	
CP-09(08)	System Backup Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined backup information].	Functional	Equal	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	10	
CP-11	Alternate Communications Protocols	Provide the capability to employ [Assignment: organization-defined alternative communications protocols] in support of maintaining continuity of operations.	Functional	Intersects With	Telecommunications Services Availability	BCD-10	Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services systems to fail to an organization-defined known-state for types of failures, preserving system state information in	5	
CP-12	Safe Mode	When [Assignment: organization-defined conditions] are detected, enter a safe mode of operation with [Assignment: organization-defined restrictions of safe mode of operation].	Functional	Intersects With	Fail Secure	SEA-07.2	Mechanisms exist to implement alternative or compensating controls to satisfy security functions when the primary means of implementing the security function is unavailable or compromised.	5	
CP-13	Alternative Security Mechanisms	Employ [Assignment: organization-defined alternative or supplemental security mechanisms] for satisfying [Assignment: organization-defined security functions] when the primary means of implementing the security function is unavailable or compromised.	Functional	Equal	Alternative Security Measures	BCD-07	Mechanisms exist to implement alternative or compensating controls to satisfy security functions when the primary means of implementing the security function is unavailable or compromised.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	of Relationships	Notes
IA-02(06)	Identification and Authentication (organizational Users) Access to Accounts — separate Device	Implement multi-factor authentication for [Selection (one or more): local; network; remote] access to [Selection (one or more): privileged accounts; non-privileged accounts] such that: a. One of the factors is provided by a device separate from the system gaining access; andb. The device meets [Assignment: organization-defined strength of mechanism requirements].	Functional	Intersects With	Out-of-Band Multi-Factor Authentication	IAC-06.4	Mechanisms exist to implement Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.	5	
IA-02(13)	Identification and Authentication (organizational Users) Out-of-band Authentication	Implement the following out-of-band authentication mechanisms under [Assignment: organization-defined conditions]: [Assignment: organization-defined out-of-band authentication].	Functional	Equal	Out-of-Band Authentication (OOBA)	IAC-02.4	Mechanisms exist to implement Out-of-Band Authentication (OOBA) under specific conditions.	10	
IA-03(01)	Device Identification and Authentication Cryptographic Bidirectional Authentication	Authenticate [Assignment: organization-defined devices and/or types of devices] before establishing [Selection (one or more): local; remote; network] connection using bidirectional authentication that is cryptographically based.	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically-based and replay resistant.	5	
IA-10	Adaptive Authentication	Require individuals accessing the system to employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific [Assignment: organization-defined circumstances or situations].	Functional	Equal	Adaptive Identification & Authentication	IAC-13	Mechanisms exist to allow individuals to utilize alternative methods of authentication under specific circumstances or situations.	10	
IR-04(02)	Incident Handling Dynamic Reconfiguration	Include the following types of dynamic reconfiguration for [Assignment: organization-defined system components] as part of the incident response capability: [Assignment: organization-defined types of dynamic reconfiguration].	Functional	Equal	Dynamic Reconfiguration	IRO-02.3	Automated mechanisms exist to dynamically reconfigure system components as part of the incident response capability.	10	
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(09)	Incident Handling Dynamic Response Capability	Employ [Assignment: organization-defined dynamic response capabilities] to respond to incidents.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
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(11)	Incident Handling Integrated Incident Response Team	Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in [Assignment: organization-defined time period].	Functional	Equal	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	10	
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	
MA-04(04)	Nonlocal Maintenance Authentication and Separation of Maintenance Sessions	Protect nonlocal maintenance sessions by: a. Employing [Assignment: organization-defined authenticators that are replay resistant]; andb. Separating the maintenance sessions from other network sessions with the system by either: 1. Physically separated communications paths; or 2. Logically separated communications paths.	Functional	Equal	Separation of Maintenance Sessions	MNT-05.7	Mechanisms exist to protect maintenance sessions through replay-resistant sessions that are physically or logically separated communications paths from other network sessions.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	of Relationships	Notes
PE-03(05)	Physical Access Control Logical Tampering Protection	Employ [Assignment: organization-defined anti-tamper technologies] to [Selection (one or more): detect; prevent] physical tampering or alteration of [Assignment: organization-defined hardware components] within the system.	Functional	Equal	Mobile Device Tampering	MDM-04	Mechanisms exist to protect mobile devices from tampering through inspecting devices returning from locations that the organization deems to be of significant risk, prior to the device being connected to the organization's network.	10	
PE-06	Monitoring Physical Access	a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; andc. Coordinate results of reviews and investigations with the organizational incident response capability.	Functional	Equal	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	10	
PE-06(02)	Monitoring Physical Access Automated Intrusion Recognition and Responses	Recognize [Assignment: organization-defined classes or types of intrusions] and initiate [Assignment: organization-defined response actions] using [Assignment: organization-defined automated mechanisms].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
PE-06(04)	Monitoring Physical Access Monitoring Physical Access to Systems	Monitor physical access to the system in addition to the physical access monitoring of the facility at [Assignment: organization-defined physical spaces containing one or more components of the system].	Functional	Equal	Monitoring Physical Access To Critical Systems	PES-05.2	Facility security mechanisms exist to monitor physical access to critical systems or sensitive/regulated data, in addition to the physical access monitoring of the facility.	10	
PE-09(01)	Power Equipment and Cabling Redundant Cabling	Employ redundant power cabling paths that are physically separated by [Assignment: organization-defined distance].	Functional	Equal	Redundant Cabling	PES-07.7	Mechanisms exist to employ redundant power cabling paths that are physically separated to ensure that power continues to flow in the event one of the cables is cut or otherwise	10	
PE-11(01)	Emergency Power Alternate Power Supply — Minimal Operational Capability	Provide an alternate power supply for the system that is activated [Selection (one): manually; automatically] and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.	Functional	Intersects With	Emergency Power	PES-07.3	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.	5	
PE-11(02)	Emergency Power Alternate Power Supply — Self-contained	Provide an alternate power supply for the system that is activated [Selection (one): manually; automatically] and that is:a. Self-contained;b. Not reliant on external power generation; andc. Capable of maintaining [Selection (one): minimally required operational capability; full operational capability] in the event of an extended loss of the primary power source.	Functional	Intersects With	Emergency Power	PES-07.3	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.	5	
PE-17	Alternate Work Site	a. Determine and document the [Assignment: organization-defined alternate work sites] allowed for use by employees;b. Employ the following controls at alternate work sites: [Assignment: organization-defined controls];c. Assess the effectiveness of controls at alternate work sites; andd. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.	Functional	Equal	Alternate Work Site	PES-11	Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.	10	
PL-08(01)	Security and Privacy Architectures Defense in Depth	Design the security and privacy architectures for the system using a defense-in-depth approach that:a. Allocates [Assignment: organization-defined controls] to [Assignment: organization-defined locations and architectural layers]; andb. Ensures that the allocated controls operate in a coordinated and mutually reinforcing manner.	Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	5	
PL-08(02)	Security and Privacy Architectures Supplier Diversity	Require that [Assignment: organization-defined controls] allocated to [Assignment: organization-defined locations and architectural layers] are obtained from different suppliers.	Functional	Intersects With	Supplier Diversity	TDA-03.1	Mechanisms exist to obtain security, compliance and resilience technologies from different suppliers to minimize supply chain risk.	5	
PM-07(01)	Enterprise Architecture Offloading	Offload [Assignment: organization-defined non-essential functions or services] to other systems, system components, or an external provider.	Functional	Equal	Outsourcing Non-Essential Functions or Services	SEA-02.2	Mechanisms exist to identify non-essential functions or services that are capable of being outsourced to external service providers and align with the organization's enterprise architecture and security requirements.	10	
PM-16	Threat Awareness Program	Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.	Functional	Intersects With	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5	
PM-16(01)	Threat Awareness Program Automated Means for Sharing Threat Intelligence Feeds	Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
PM-30(01)	Supply Chain Risk Management Strategy Suppliers of Critical or Mission-essential	Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.	Functional	Intersects With	Customized Development of Critical Components	TDA-12	Mechanisms exist to custom-develop critical system components, when Commercial Off The Shelf (COTS) solutions are unavailable.	5	
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 (SDLCL).	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	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	of Relationships	Notes
PM-32	Purposing	Analyze [Assignment: organization-defined systems or systems components] supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose.	Functional	Equal	Purpose Validation	GOV-11	Mechanisms exist to monitor mission/business-critical Technology Assets, Applications and/or Services (TAAS) to ensure those resources are being used consistent with their intended purpose.	10	
RA-03(02)	Risk Assessment Use of All-source Intelligence	Use all-source intelligence to assist in the analysis of risk.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
RA-03(03)	Risk Assessment Dynamic Threat Awareness	Determine the current cyber threat environment on an ongoing basis using [Assignment: organization-defined means].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
RA-03(04)	Risk Assessment Predictive Cyber Analytics	Employ the following advanced automation and analytics capabilities to predict and identify risks to [Assignment: organization-defined systems or system components]; [Assignment: organization-defined advanced automation and analytics capabilities].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
RA-05(04)	Vulnerability Monitoring and Scanning Discoverable Information	Determine information about the system that is discoverable and take [Assignment: organization-defined corrective actions].	Functional	Equal	Acceptable Discoverable Information	VPM-06.8	Mechanisms exist to define what information is allowed to be discoverable by adversaries and take corrective actions to remediate non-compliant Technology Assets, Applications	10	
RA-05(05)	Vulnerability Monitoring and Scanning Privileged Access	Implement privileged access authorization to [Assignment: organization-defined system components] for [Assignment: organization-defined vulnerability scanning activities].	Functional	Equal	Privileged Access	VPM-06.3	Mechanisms exist to implement privileged access authorization for selected vulnerability scanning activities.	10	
RA-05(06)	Vulnerability Monitoring and Scanning Automated Trend Analyses	Compare the results of multiple vulnerability scans using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Trend Analysis	VPM-06.4	Automated mechanisms exist to compare the results of vulnerability scans over time to determine trends in system vulnerabilities.	10	
RA-05(08)	Vulnerability Monitoring and Scanning Review Historic Audit Logs	Review historic audit logs to determine if a vulnerability identified in a [Assignment: organization-defined system] has been previously exploited within an [Assignment: organization-defined time period].	Functional	Equal	Review Historical Event logs	VPM-06.5	Mechanisms exist to review historical event logs to determine if identified vulnerabilities have been previously exploited.	10	
RA-05(10)	Vulnerability Monitoring and Scanning Correlate Scanning Information	Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors.	Functional	Equal	Correlate Scanning Information	VPM-06.9	Automated mechanisms exist to correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.	10	
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	
RA-10	Threat Hunting	a. Establish and maintain a cyber threat hunting capability to:1. Search for indicators of compromise in organizational systems; and2. Detect, track, and disrupt threats that evade existing controls; andb. Employ the threat hunting capability [Assignment: organization-defined frequency].	Functional	Equal	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses indicators of compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	10	
SA-03(02)	System Development Life Cycle Use of Live or Operational Data	a. Approve, document, and control the use of live data in preproduction environments for the system, system component, or system service; andb. Protect preproduction environments for the system, system component, or system service at the same impact or classification level as any live data in use within the preproduction environments.	Functional	Equal	Use of Live Data	TDA-10	Mechanisms exist to approve, document and control the use of live data in development and test environments.	10	
SA-08(02)	Privacy Engineering Principles Least Common Mechanism	Implement the security design principle of least common mechanism in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SA-08(03)	Privacy Engineering Principles Modularity and Security and	Implement the security design principles of modularity and layering in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SA-08(04)	Privacy Engineering Principles Partially Ordered Dependencies and Security and	Implement the security design principle of partially ordered dependencies in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SA-08(06)	Privacy Engineering Principles Minimized Sharing and Security and	Implement the security design principle of minimized sharing in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SA-08(07)	Privacy Engineering Principles Reduced Complexity and Security and	Implement the security design principle of reduced complexity in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SA-08(08)	Privacy Engineering Principles Secure Evolvability and Security and	Implement the security design principle of secure evolvability in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SA-08(13)	Privacy Engineering Principles Minimized Security Elements	Implement the security design principle of minimized security elements in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SA-08(15)	Privacy Engineering Principles Predicate	Implement the security design principle of predicate permission in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SA-08(16)	Security and Privacy Engineering Principles Self-reliant Trustworthiness and Security and	Implement the security design principle of self-reliant trustworthiness in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SA-08(17)	Privacy Engineering Principles Secure Distributed Composition	Implement the security design principle of secure distributed composition in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SA-08(18)	Security and Privacy Engineering Principles Trusted Communications Channels	Implement the security design principle of trusted communications channels in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SA-08(19)	Privacy Engineering Principles Continuous	Implement the security design principle of continuous protection in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	of Relationships	Notes
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-09(07)	External System Services Organization-controlled Integrity Checking	Provide the capability to check the integrity of information while it resides in the external system.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SA-11(02)	Developer Testing and Evaluation Threat Modeling and Vulnerability Analyses	Require the developer or 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]; and d. Produces evidence that meets the following acceptance criteria: [Assignment: organization-defined acceptance criteria].	Functional	Intersects With	Threat Analysis & Flaw Remediation	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 proactively identify and remediate vulnerabilities prior to release to production.	5	
SA-11(02)	Developer Testing and Evaluation Threat Modeling and Vulnerability Analyses	Require the developer or 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]; and d. 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]; and b. 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]; and b. 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]; and b. 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]; and b. 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]; and b. 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	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	of Relationships	Notes
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	
SA-17(06)	Developer Security and Privacy Architecture and Design Structure for Testing	Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate testing.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SA-17(08)	Developer Security and Privacy Architecture and Design Orchestration	Design [Assignment: organization-defined critical systems or system components] with coordinated behavior to implement the following capabilities: [Assignment: organization-defined capabilities, by system or component].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SA-17(09)	Developer Security and Privacy Architecture and Design Design Diversity	Use different designs for [Assignment: organization-defined critical systems or system components] to satisfy a common set of requirements or to provide equivalent functionality.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SA-20	Customized Development of Critical Components	Reimplement or custom develop the following critical system components: [Assignment: organization-defined critical system components].	Functional	Equal	Customized Development of Critical Components	TDA-12	Mechanisms exist to custom-develop critical system components, when Commercial Off The Shelf (COTS) solutions are unavailable.	10	
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-02	Separation of System and User Functionality	Separate user functionality, including user interface services, from system management functionality.	Functional	Equal	Application Partitioning	SEA-03.2	Mechanisms exist to separate user functionality from system management functionality.	10	
SC-02(01)	Separation of System and User Functionality Interfaces for Non-privileged Users	Prevent the presentation of system management functionality at interfaces to non-privileged users.	Functional	Equal	Application Partitioning	SEA-03.2	Mechanisms exist to separate user functionality from system management functionality.	10	
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-03(01)	Security Function Isolation Hardware Separation	Employ hardware separation mechanisms to implement security function isolation.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SC-03(02)	Security Function Isolation Access and Flow Control Functions	Isolate security functions enforcing access and information flow control from nonsecurity functions and from other security functions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SC-03(03)	Security Function Isolation Minimize Nonsecurity Functionality	Minimize the number of nonsecurity functions included within the isolation boundary containing security functions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SC-03(05)	Security Function Isolation Layered Structures	Implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	Functional	Equal	Defense-In-Depth (DID) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	10	
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-05(03)	Denial-of-service Protection Detection and Monitoring	a. Employ the following monitoring tools to detect indicators of denial-of-service attacks against, or launched from, the system: [Assignment: organization-defined monitoring tools]; andb. Monitor the following system resources to determine if sufficient resources exist to prevent effective denial-of-service attacks: [Assignment: organization-defined system resources]. a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system.b. Implement subnetworks for publicly accessible system components that are [Selection (one): physically; logically] separated from internal organizational networks; andc. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.	Functional	Intersects With	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-07	Boundary Protection	a. Prevent the exfiltration of information; andb. Conduct exfiltration tests [Assignment: organization-defined frequency].	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(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	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	of Relationships	Notes
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(13)	Boundary Protection Isolation of Security Tools, Mechanisms, and Support Components	Isolate [Assignment: organization-defined information security tools, mechanisms, and support components] from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.	Functional	Intersects With	Security Management Subnets	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the system.	5	
SC-07(15)	Boundary Protection Networked Privileged Accesses	Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.	Functional	Equal	Route Privileged Network Access	NET-18.3	Automated mechanisms exist to route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.	10	
SC-07(16)	Protection Prevent Discovery of System	Prevent the discovery of specific system components that represent a managed interface.	Functional	Equal	Prevent Discovery of Internal Information	NET-03.3	Mechanisms exist to prevent the public disclosure of internal network information.	10	
SC-07(20)	Boundary Protection Dynamic Isolation and Segregation	Provide the capability to dynamically isolate [Assignment: organization-defined system components] from other system components.	Functional	Equal	Dynamic Isolation & Segregation (Sandboxing)	NET-03.6	Automated mechanisms exist to dynamically isolate (e.g., sandbox) untrusted components during runtime, where the component is isolated in a fault-contained environment but it can still collaborate with the application.	10	
SC-07(21)	Boundary Protection Isolation of System Components	Employ boundary protection mechanisms to isolate [Assignment: organization-defined system components] supporting [Assignment: organization-defined missions and/or business functions].	Functional	Equal	Isolation of System Components	NET-03.7	Mechanisms exist to employ boundary protections to isolate Technology Assets, Applications and/or Services (TAAS) that support critical missions and/or business functions.	10	
SC-07(22)	Protection Separate Subnets for Connecting to Different Security Domains	Implement separate network addresses to connect to systems in different security domains.	Functional	Intersects With	Separate Subnet for Connecting to Different Security Domains	NET-03.8	Mechanisms exist to implement separate network addresses (e.g., different subnets) to connect to systems in different security domains.	5	
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(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(04)	Transmission Confidentiality and Integrity Conceal or Randomize Communications	Implement cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by [Assignment: organization-defined alternative physical controls].	Functional	Equal	Conceal / Randomize Communications	CRY-01.4	Cryptographic mechanisms exist to conceal or randomize communication patterns.	10	
SC-08(05)	Transmission Confidentiality and Integrity Protected Distribution System	Implement [Assignment: organization-defined protected distribution system] to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SC-10	Network Disconnect	Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.	Functional	Equal	Network Connection Termination	NET-07	Mechanisms exist to terminate network connections at the end of a session or after an organization-defined time period of inactivity.	10	
SC-11	Trusted Path	a. Provide a [Selection (one): physically; logically] isolated trusted communications path for communications between the user and the trusted components of the system; andb. Permit users to invoke the trusted communications path for communications between the user and the following security functions of the system, including at a minimum, authentication and re-authentication: [Assignment: organization-defined security functions].	Functional	Equal	Trusted Path	END-09	Mechanisms exist to establish a trusted communications path between the user and the security functions of the operating system.	10	
SC-15(01)	Collaborative Computing Devices and Applications Physical or Logical Disconnect	Provide [Selection (one or more): physical; logical] disconnect of collaborative computing devices in a manner that supports ease of use.	Functional	Intersects With	Collaborative Computing Devices	END-14	Mechanisms exist to unplug or prohibit the remote activation of collaborative computing devices with the following exceptions: (1) Networked whiteboards; (2) Video teleconference cameras; and (3) Teleconference microphones.	5	
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-16(03)	Transmission of Security and Privacy Attributes Cryptographic Binding	Implement [Assignment: organization-defined mechanisms or techniques] to bind security and privacy attributes to transmitted information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SC-18(05)	Mobile Code Allow Execution Only in Confined Environments	Allow execution of permitted mobile code only in confined virtual machine environments.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	of Relationships	Notes
SC-22	Architecture and Provisioning for Name/Address Resolution Service	Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.	Functional	Equal	Architecture & Provisioning for Name / Address Resolution Service	NET-10.1	Mechanisms exist to ensure systems that collectively provide Domain Name Service (DNS) resolution service are fault-tolerant and implement internal/external role separation.	10	
SC-23(03)	Session Authenticity Unique System-generated Session Identifiers	Generate a unique session identifier for each session with [Assignment: organization-defined randomness requirements] and recognize only session identifiers that are system-generated.	Functional	Equal	Unique System-Generated Session Identifiers	NET-09.2	Automated mechanisms exist to generate and recognize unique session identifiers for each session.	10	
SC-25	Thin Nodes	Employ minimal functionality and information storage on the following system components: [Assignment: organization-defined system components].	Functional	Equal	Thin Nodes	END-11	Mechanisms exist to configure thin nodes to have minimal functionality and information storage.	10	
SC-26	Decoys	Include components within organizational systems specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.	Functional	Equal	Honey pots	SEA-11	Mechanisms exist to utilize honeypots that are specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting and analyzing such attacks.	10	
SC-27	Platform-independent Applications	Include within organizational systems the following platform independent applications: [Assignment: organization-defined platform-independent applications].	Functional	Equal	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	10	
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-29	Heterogeneity	Employ a diverse set of information technologies for the following system components in the implementation of the system: [Assignment: organization-defined system components].	Functional	Equal	Heterogeneity	SEA-13	Mechanisms exist to utilize a diverse set of technologies for system components to reduce the impact of technical vulnerabilities from the same Original Equipment Manufacturer.	10	
SC-29(01)	Heterogeneity Virtualization Techniques	Employ virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [Assignment: organization-defined frequency].	Functional	Equal	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	10	
SC-30	Concealment and Misdirection	Employ the following concealment and misdirection techniques for [Assignment: organization-defined systems] at [Assignment: organization-defined time periods] to confuse and mislead adversaries: [Assignment: organization-defined concealment and misdirection techniques].	Functional	Intersects With	Concealment & Misdirection	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for Technology Assets, Applications and/or Services (TAAS) to confuse and mislead adversaries.	5	
SC-30(02)	Concealment and Misdirection Randomness	Employ [Assignment: organization-defined techniques] to introduce randomness into organizational operations and assets.	Functional	Equal	Randomness	SEA-14.1	Automated mechanisms exist to introduce randomness into organizational operations and assets.	10	
SC-30(03)	Concealment and Misdirection Change Processing and Storage Locations	Change the location of [Assignment: organization-defined processing and/or storage] [Selection (one): [Assignment: organization-defined time frequency]; at random time intervals].	Functional	Equal	Change Processing & Storage Locations	SEA-14.2	Automated mechanisms exist to change the location of processing and/or storage at random time intervals.	10	
SC-30(04)	Concealment and Misdirection Misleading Information	Employ realistic, but misleading information in [Assignment: organization-defined system components] about its security state or posture.	Functional	Intersects With	Concealment & Misdirection	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for Technology Assets, Applications and/or Services (TAAS) to confuse and mislead adversaries.	5	
SC-30(05)	Concealment and Misdirection Concealment of System Components	Employ the following techniques to hide or conceal [Assignment: organization-defined system components]: [Assignment: organization-defined techniques].	Functional	Intersects With	Concealment & Misdirection	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for Technology Assets, Applications and/or Services (TAAS) to confuse and mislead adversaries.	5	
SC-32	System Partitioning	Partition the system into [Assignment: organization-defined system components] residing in separate [Selection (one): physical; logical] domains or environments based on [Assignment: organization-defined circumstances for physical or logical separation of components].	Functional	Equal	System Partitioning	SEA-03.1	Mechanisms exist to partition systems so that partitions reside in separate physical domains or environments.	10	
SC-32(01)	System Partitioning Separate Physical Domains for Privileged Functions	Partition privileged functions into separate physical domains.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SC-34	Non-modifiable Executable Programs	For [Assignment: organization-defined system components], load and execute: The operating environment from hardware-enforced, read-only media; andb. The following applications from hardware-enforced, read-only media: [Assignment: organization-defined applications].	Functional	Equal	Non-Modifiable Executable Programs	SEA-16	Mechanisms exist to utilize non-modifiable executable programs that load and execute the operating environment and applications from hardware-enforced, read-only media.	10	
SC-34(01)	Non-modifiable Executable Programs No Writable Storage	Employ [Assignment: organization-defined system components] with no writable storage that is persistent across component restart or power on/off.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SC-34(02)	Non-modifiable Executable Programs Integrity Protection on Read-only Media	Protect the integrity of information prior to storage on read-only media and control the media after such information has been recorded onto the media.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SC-35	External Malicious Code Identification	Include system components that proactively seek to identify network-based malicious code or malicious websites.	Functional	Equal	Honeyclients	SEA-12	Mechanisms exist to utilize honeyclients that proactively seek to identify malicious websites and/or web-based malicious code.	10	
SC-36	Distributed Processing and Storage	Distribute the following processing and storage components across multiple [Selection (one): physical locations; logical domains]: [Assignment: organization-defined processing and storage components].	Functional	Equal	Distributed Processing & Storage	SEA-15	Mechanisms exist to distribute processing and storage across multiple physical locations.	10	
SC-36(01)	Distributed Processing and Storage Polling Techniques	a. Employ polling techniques to identify potential faults, errors, or compromises to the following processing and storage components: [Assignment: organization-defined distributed processing and storage components]; andb. Take the following actions in response to identified faults, errors, or compromises: [Assignment: organization-defined actions].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SC-36(02)	Distributed Processing and Storage Synchronization	Synchronize the following duplicate systems or system components: [Assignment: organization-defined duplicate systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SC-37	Out-of-band Channels	Employ the following out-of-band channels for the physical delivery or electronic transmission of [Assignment: organization-defined information, system components, or devices] to [Assignment: organization-defined individuals or systems]: [Assignment: organization-defined out-of-band channels].	Functional	Intersects With	Out-of-Band Channels	NET-11	Mechanisms exist to utilize out-of-band channels for the electronic transmission of information and/or the physical shipment of system components or devices to authorized individuals.	5	
SC-39	Process Isolation	Maintain a separate execution domain for each executing system process.	Functional	Equal	Process Isolation	SEA-04	Mechanisms exist to implement a separate execution domain for each executing process.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	of Relationships	Notes
SC-39(01)	Process Isolation Hardware Separation	Implement hardware separation mechanisms to facilitate process isolation.	Functional	Equal	Hardware Separation	SEA-04.2	Mechanisms exist to implement underlying hardware separation mechanisms to facilitate process separation.	10	
SC-39(02)	Process Isolation Separate Execution Domain Per Thread	Maintain a separate execution domain for each thread in [Assignment: organization-defined multi-threaded processing].	Functional	Equal	Thread Separation	SEA-04.3	Mechanisms exist to maintain a separate execution domain for each thread in multi-threaded processing.	10	
SC-40(02)	Wireless Link Protection Reduce Detection Potential	Implement cryptographic mechanisms to reduce the detection potential of wireless links to [Assignment: organization-defined level of reduction].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SC-40(03)	Wireless Link Protection Imitative or Manipulative Communications Deception	Implement cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SC-44	Detonation Chambers	Employ a detonation chamber capability within [Assignment: organization-defined system, system component, or location].	Functional	Equal	Detonation Chambers (Sandboxes)	IRO-15	Mechanisms exist to utilize a detonation chamber capability to detect and/or block potentially-malicious files and email attachments.	10	
SC-46	Cross Domain Policy Enforcement	Implement a policy enforcement mechanism [Selection (one): physically; logically] between the physical and/or network interfaces for the connecting security domains.	Functional	Equal	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	10	
SC-47	Alternate Communications Channels	Establish [Assignment: organization-defined alternate communications paths] for system operations organizational command and control.	Functional	Equal	Alternate Communications Channels	BCD-10.4	Mechanisms exist to maintain command and control capabilities via alternate communications channels and designating alternative decision makers if primary decision makers are unavailable.	10	
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	
SC-48(01)	Sensor Relocation Dynamic Relocation of Sensors or Monitoring Capabilities	Dynamically relocate [Assignment: organization-defined sensors and monitoring capabilities] to [Assignment: organization-defined locations] under the following conditions or circumstances: [Assignment: organization-defined conditions or circumstances].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SC-49	Hardware-enforced Separation and Policy Enforcement	Implement hardware-enforced separation and policy enforcement mechanisms between [Assignment: organization-defined security domains].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SC-50	Software-enforced Separation and Policy Enforcement	Implement software-enforced separation and policy enforcement mechanisms between [Assignment: organization-defined security domains].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SC-51	Hardware-based Protection	a. Employ hardware-based, write-protect for [Assignment: organization-defined system firmware components]; and b. Implement specific procedures for [Assignment: organization-defined authorized individuals] to manually disable hardware write-protect for firmware modifications and re-enable the write-protect prior to returning to operational mode.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SI-03(10)	Malicious Code Protection Malicious Code Analysis	a. Employ the following tools and techniques to analyze the characteristics and behavior of malicious code: [Assignment: organization-defined tools and techniques]; and b. Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SI-04(01)	System Monitoring System-wide Intrusion Detection System	Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.	Functional	Equal	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	10	
SI-04(02)	System Monitoring Automated Tools and Mechanisms for Real-time Analysis	Employ automated tools and mechanisms to support near real-time analysis of events.	Functional	Equal	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	10	
SI-04(03)	System Monitoring Automated Tool and Mechanism Integration	Employ automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access control and flow control mechanisms.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SI-04(04)	System Monitoring Inbound and Outbound Communications Traffic	a. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic; [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].	Functional	Equal	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	10	
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; and b. 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; and b. 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(10)	System Monitoring Visibility of Encrypted Communications	Make provisions so that [Assignment: organization-defined encrypted communications traffic] is visible to [Assignment: organization-defined system monitoring tools and mechanisms].	Functional	Equal	Visibility of Encrypted Communications	NET-18.2	Mechanisms exist to configure the proxy to make encrypted communications traffic visible to monitoring tools and mechanisms.	10	
SI-04(11)	System Monitoring Analyze Communications Traffic Anomalies	Analyze outbound communications traffic at the external interfaces to the system and selected [Assignment: organization-defined interior points within the system] to discover anomalies.	Functional	Equal	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	10	
SI-04(13)	System Monitoring Analyze Traffic and Event Patterns	a. Analyze communications traffic and event patterns for the system; b. Develop profiles representing common traffic and event patterns; and c. Use the traffic and event profiles in tuning system-monitoring devices.	Functional	Equal	Alert Threshold Tuning	MON-01.13	Mechanisms exist to "tune" event monitoring technologies through analyzing communications traffic/event patterns and developing profiles representing common traffic patterns and/or events.	10	
SI-04(16)	System Monitoring Correlate Monitoring Information	Correlate information from monitoring tools and mechanisms employed throughout the system.	Functional	Equal	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	of Relationships	Notes
SI-04(17)	System Monitoring Integrated Situational Awareness	Correlate information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.	Functional	Equal	Integration of Scanning & Other Monitoring Information	MON-02.3	Automated mechanisms exist to integrate the analysis of audit records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further enhance the ability to identify inappropriate or unusual activity.	10	
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-06	Security and Privacy Function Verification	a. Verify the correct operation of [Assignment: organization-defined security and privacy functions]; b. Perform the verification of the functions specified in SI-06a [Selection (one or more); [Assignment: organization-defined system transitional states], upon command by user with appropriate privilege; [Assignment: organization-defined frequency]]; c. Alert [Assignment: organization-defined personnel or roles] to failed security and privacy verification tests; and d. [Selection (one or more): Shut the system down; Restart the system; [Assignment: organization-defined alternative action(s)] when anomalies are discovered.	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	5	
SI-07	Software, Firmware, and Information Integrity	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; and b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].	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]; and b. 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]; and b. 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-07(01)	Software, Firmware, and Information Integrity Integrity Checks	Perform an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]].	Functional	Equal	Integrity Checks	END-06.1	Mechanisms exist to validate configurations through integrity checking of software and firmware.	10	
SI-07(05)	Software, Firmware, and Information Integrity Automated Response to Integrity Violations	Automatically [Selection (one or more): shut the system down; restart the system; implement [Assignment: organization-defined controls]] when integrity violations are discovered.	Functional	Equal	Automated Response to Integrity Violations	END-06.4	Automated mechanisms exist to implement remediation actions when integrity violations are discovered.	10	
SI-07(06)	Software, Firmware, and Information Integrity Cryptographic Protection	Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.	Functional	Equal	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
SI-07(07)	Software, Firmware, and Information Integrity Integration of Detection and Response	Incorporate the detection of the following unauthorized changes into the organizational incident response capability: [Assignment: organization-defined security-relevant changes to the system].	Functional	Equal	Endpoint Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.	10	
SI-07(09)	Software, Firmware, and Information Integrity Verify Boot Process	Verify the integrity of the boot process of the following system components: [Assignment: organization-defined system components].	Functional	Equal	Boot Process Integrity	END-06.5	Automated mechanisms exist to verify the integrity of the boot process of systems.	10	
SI-07(10)	Software, Firmware, and Information Integrity Protection of Boot Firmware	Implement the following mechanisms to protect the integrity of boot firmware in [Assignment: organization-defined system components]: [Assignment: organization-defined mechanisms].	Functional	Equal	Protection of Boot Firmware	END-06.6	Automated mechanisms exist to protect the integrity of boot firmware in systems.	10	
SI-07(12)	Software, Firmware, and Information Integrity Integrity Verification	Require that the integrity of the following user-installed software be verified prior to execution: [Assignment: organization-defined user-installed software].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SI-07(15)	Software, Firmware, and Information Integrity Code Authentication	Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: [Assignment: organization-defined software or firmware components].	Functional	Intersects With	Signed Components	CHG-04.2	Mechanisms exist to prevent the installation of software and firmware components without verification that the component has been digitally signed using an organization-approved certificate authority.	5	
SI-10(03)	Information Input Validation Predictable Behavior	Verify that the system behaves in a predictable and documented manner when invalid inputs are received.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SI-10(05)	Information Input Validation Restrict Inputs to Trusted Sources and Approved Formats	Restrict the use of information inputs to [Assignment: organization-defined trusted sources] and/or [Assignment: organization-defined formats].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SI-14	Non-persistence	Implement non-persistent [Assignment: organization-defined system components and services] that are initiated in a known state and terminated [Selection (one or more): upon end of session of use; periodically at [Assignment: organization-defined frequency]].	Functional	Equal	Non-Persistence	SEA-08	Mechanisms exist to implement non-persistent system components and services that are initiated in a known state and terminated upon the end of the session of use or periodically at an organization-defined frequency.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	of Relationships	Notes
SI-14(01)	Non-persistence Refresh from Trusted Sources	Obtain software and data employed during system component and service refreshes from the following trusted sources: [Assignment: organization-defined trusted sources].	Functional	Equal	Refresh from Trusted Sources	SEA-08.1	Mechanisms exist to ensure that software and data needed for system component and service refreshes are obtained from trusted sources.	10	
SI-14(02)	Non-persistence Non-persistent Information	a. [Selection (one): Refresh [Assignment: organization-defined information] [Assignment: organization-defined frequency]; Generate [Assignment: organization-defined information] on demand; andb. Delete information when no longer needed.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SI-14(03)	Non-persistence Non-persistent Connectivity	Establish connections to the system on demand and terminate connections after [Selection (one): completion of a request; a period of non-use].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SI-15	Information Output Filtering	Validate information output from the following software programs and/or applications to ensure that the information is consistent with the expected content: [Assignment: organization-defined software programs and/or applications].	Functional	Equal	Information Output Filtering	SEA-09	Mechanisms exist to validate information output from software programs and/or applications to ensure that the information is consistent with the expected content.	10	
SI-16	Memory Protection	Implement the following controls to protect the system memory from unauthorized code execution: [Assignment: organization-defined controls].	Functional	Equal	Memory Protection	SEA-10	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	10	
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	
SI-19(06)	De-identification Differential Privacy	Prevent disclosure of personally identifiable information by adding non-deterministic noise to the results of mathematical operations before the results are reported.	Functional	Equal	Differential Data Privacy	DCH-23.6	Mechanisms exist to prevent disclosure of Personal Data (PD) by adding non-deterministic noise to the results of mathematical operations before the results are reported.	10	
SI-19(08)	De-identification Motivated Intruder	Perform a motivated intruder test on the de-identified dataset to determine if the identified data remains or if the de-identified data can be re-identified.	Functional	Equal	Motivated Intruder	DCH-23.8	Mechanisms exist to perform a motivated intruder test on the de-identified dataset to determine if the identified data remains or if the de-identified data can be re-identified.	10	
SI-20	Tainting	Embed data or capabilities in the following systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization: [Assignment: organization-defined systems or system components].	Functional	Equal	Tainting	THR-08	Mechanisms exist to embed data or steganographic data in files to enable the organization to determine if data has been exfiltrated and provide a means to identify the individual(s) involved.	10	
SI-21	Information Refresh	Refresh [Assignment: organization-defined information] at [Assignment: organization-defined frequencies] or generate the information on demand and delete the information when no longer needed.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SI-22	Information Diversity	a. Identify the following alternative sources of information for [Assignment: organization-defined essential functions and services]: [Assignment: organization-defined alternative information sources]; andb. Use an alternative information source for the execution of essential functions or services on [Assignment: organization-defined systems or system components] when the primary source of information is unavailable.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SI-23	Information Fragmentation	a. Fragment the following information: [Assignment: organization-defined information]; andb. Distribute the fragmented information across the following systems or system components: [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
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(02)	Supply Chain Controls and Processes Limitation of Harm	Employ the following controls to limit harm from potential adversaries identifying and targeting the organizational supply chain: [Assignment: organization-defined controls].	Functional	Equal	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	10	
SR-04	Provenance	Document, monitor, and maintain valid provenance of the following systems, system components, and associated data: [Assignment: organization-defined systems, system components, and associated data].	Functional	Intersects With	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to Technology Assets, Applications, Services and/or Data (TAASD).	5	
SR-04(01)	Provenance Identity	Establish and maintain unique identification of the following supply chain elements, processes, and personnel associated with the identified system and critical system components: [Assignment: organization-defined supply chain elements, processes, and personnel associated with organization-defined systems and critical system components].	Functional	Intersects With	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to Technology Assets, Applications, Services and/or Data (TAASD).	5	
SR-04(02)	Provenance Track and Trace	Establish and maintain unique identification of the following systems and critical system components for tracking through the supply chain: [Assignment: organization-defined systems and critical system components].	Functional	Intersects With	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to Technology Assets, Applications, Services and/or Data (TAASD).	5	
SR-04(03)	Provenance Validate as Genuine and Not Altered	Employ the following controls to validate that the system or system component received is genuine and has not been altered: [Assignment: organization-defined controls].	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5	
SR-04(04)	Provenance Supply Chain Integrity — Pedigree	Employ [Assignment: organization-defined controls] and conduct [Assignment: organization-defined analysis] to ensure the integrity of the system and system components by validating the internal composition and provenance of critical or mission-essential technologies, products, and services.	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	of Relationships	Notes
SR-05	Acquisition Strategies, Tools, and Methods	Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined acquisition strategies, contract tools, and procurement methods].	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services.	5	
SR-05(01)	Acquisition Strategies, Tools, and Methods Adequate Supply	Employ the following controls to ensure an adequate supply of [Assignment: organization-defined critical system components]: [Assignment: organization-defined controls].	Functional	Equal	Adequate Supply	TPM-03.4	Mechanisms exist to develop and implement a spare parts strategy to ensure that an adequate supply of critical components is available to meet operational needs.	10	
SR-06(01)	Supplier Assessments and Reviews Testing and Analysis	Employ [Selection (one or more): organizational analysis; independent third-party analysis; organizational testing; independent third-party testing] of the following supply chain elements, processes, and actors associated with the system, system component, or system service: [Assignment: organization-defined supply chain elements, processes, and actors].	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5	
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 risks.	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-09	Tamper Resistance and Detection	Implement a tamper protection program for the system, system component, or system service.	Functional	Intersects With	Logical Tampering Protection	AST-15	Mechanisms exist to assess the integrity of critical Technology Assets, Applications and/or Services (TAAS) to detect evidence of tampering, where: (1) Logical assessments evaluate the integrity of critical components (e.g., configuration settings); and (2) Physical assessments evaluate assets for evidence of unauthorized access and/or tampering.	5	
SR-09(01)	Tamper Resistance and Detection Multiple Stages of System Development Life Cycle	Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle.	Functional	Intersects With	Logical Tampering Protection	AST-15	Mechanisms exist to assess the integrity of critical Technology Assets, Applications and/or Services (TAAS) to detect evidence of tampering, where: (1) Logical assessments evaluate the integrity of critical components (e.g., configuration settings); and (2) Physical assessments evaluate assets for evidence of unauthorized access and/or tampering.	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	
SR-11	Component Authenticity	a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and b. Report counterfeit system components to [Selection (one or more): source of counterfeit component; [Assignment: organization-defined external reporting organizations]; [Assignment: organization-defined personnel or roles]].	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-11(03)	Component Authenticity Anti-counterfeit Scanning	Scan for counterfeit system components [Assignment: organization-defined frequency].	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5	