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

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

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Relationsh | Notes |
|---|---|---|---|---|---|---|---|---|---|
| AC-02(11) | Account Management \| Usage Conditions | Enforce [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined system accounts]. | Functional | Equal | Usage Conditions | IAC-15.8 | Automated mechanisms exist to enforce usage conditions for users and/or roles. | 10 | |
| 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-04(04) | Information Flow Enforcement \| Flow Control of Encrypted Information | Prevent encrypted information from bypassing [Assignment: organization-defined information flow control mechanisms] by [Selection (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information; [Assignment: organization-defined procedure or method]]. | Functional | Equal | Content Check for Encrypted Data | NET-04.3 | Mechanisms exist to prevent encrypted data from bypassing content-checking mechanisms. | 10 | |
| 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-10 | Concurrent Session Control | Limit the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number]. | Functional | Equal | Concurrent Session Control | IAC-23 | Mechanisms exist to limit the number of concurrent sessions for each system account. | 10 | |
| AC-18(04) | Wireless Access \| Restrict Configurations by Users | Identify and explicitly authorize users allowed to independently configure wireless networking capabilities. | Functional | Equal | Restrict Configuration By Users | NET-15.3 | Mechanisms exist to identify and explicitly authorize users who are allowed to independently configure wireless networking capabilities. | 10 | |
| AC-18(05) | Wireless Access \| Antennas and Transmission Power Levels | Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries. | Functional | Equal | Wireless Boundaries | NET-15.4 | Mechanisms exist to confine wireless communications to organization-controlled boundaries. | 10 | |
| AU-05(01) | Response to Audit Logging Process Failures \| Storage Capacity Warning | Provide a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated audit log storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit log storage capacity. | Functional | Equal | Event Log Storage Capacity Alerting | MON-05.2 | Automated mechanisms exist to alert appropriate personnel when the allocated volume reaches an organization-defined percentage of maximum event log storage capacity. | 10 | |
| AU-05(02) | Response to Audit Logging Process Failures \| Real-time Alerts | Provide an alert within [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit logging failure events requiring real-time alerts]. | Functional | Intersects With | Real-Time Alerts of Event Logging Failure | MON-05.1 | Mechanisms exist to provide 24x7x365 near real-time alerting capability when an event log processing failure occurs. | 5 | |
| 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-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-10 | Non-repudiation | Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [Assignment: organization-defined actions to be covered by non-repudiation]. | Functional | Equal | Non-Repudiation | MON-09 | Mechanisms exist to utilize a non-repudiation capability to protect against an individual falsely denying having performed a particular action. | 10 | |
| AU-12(01) | Audit Record Generation \| System-wide and Time-correlated Audit Trail | Compile audit records from [Assignment: organization-defined system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail]. | Functional | Equal | System-Wide / Time-Correlated Audit Trail | MON-02.7 | Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated. | 10 | |
| AU-12(03) | Audit Record Generation \| Changes by Authorized Individuals | Provide and implement the capability for [Assignment: organization-defined individuals or roles] to change the logging to be performed on [Assignment: organization-defined system components] based on [Assignment: organization-defined selectable event criteria] within [Assignment: organization-defined time thresholds]. | Functional | Equal | Changes by Authorized Individuals | MON-02.8 | Mechanisms exist to provide privileged users or roles the capability to change the auditing to be performed on specified system components, based on specific event criteria within specified time thresholds. | 10 | |
| CA-02(02) | Control Assessments \| Specialized Assessments | Include as part of control assessments, [Assignment: organization-defined frequency], [Selection (one): announced; unannounced], [Selection (one or more): in-depth monitoring; security instrumentation; automated security test cases; vulnerability scanning; malicious user testing; insider threat assessment; performance and load testing; data leakage or data loss assessment; [Assignment: organization-defined other forms of assessment]]. | Functional | Intersects With | Specialized Assessments | IAO-02.2 | Mechanisms exist to conduct specialized assessments for:<br>(1) Statutory, regulatory and contractual compliance obligations;<br>(2) Monitoring capabilities;<br>(3) Mobile devices;<br>(4) Databases;<br>(5) Application security;<br>(6) Embedded technologies (e.g., IoT, OT, etc.);<br>(7) Vulnerability management;<br>(8) Malicious code;<br>(9) Insider threats;<br>(10) Performance/load testing; and/or<br>(11) Artificial Intelligence and Autonomous Technologies (AAT). | 5 | |
| CA-03(06) | Information Exchange \| Transfer Authorizations | Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data. | Functional | Equal | Transfer Authorizations | DCH-14.2 | Mechanisms exist to verify that individuals or Technology Assets, Applications and/or Services (TAAS) transferring data between interconnecting TAAS have the requisite authorizations (e.g., write permissions or privileges) prior to transferring said data. | 10 | |

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationsh | Notes |
|---|---|---|---|---|---|---|---|---|---|
| CA-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 | |
| CM-03(01) | Configuration Change Control \| Automated Documentation, Notification, and Prohibition of Changes | Use [Assignment: organization-defined automated mechanisms] to:a. Document proposed changes to the system;b. Notify [Assignment: organization-defined approval authorities] of proposed changes to the system and request change approval;c. Highlight proposed changes to the system that have not been approved or disapproved within [Assignment: organization-defined time period];d. Prohibit changes to the system until designated approvals are received;e. Document all changes to the system; andf. Notify [Assignment: organization-defined personnel] when approved changes to the system are completed. | Functional | Equal | Prohibition Of Changes | CHG-02.1 | Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received. | 10 | |
| CM-03(06) | Configuration Change Control \| Cryptography Management | Ensure that cryptographic mechanisms used to provide the following controls are under configuration management: [Assignment: organization-defined controls]. | Functional | Equal | Cryptographic Management | CHG-02.5 | Mechanisms exist to govern assets involved in providing cryptographic protections according to the organization's configuration management processes. | 10 | |
| 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(01) | Access Restrictions for Change \| Automated Access Enforcement and Audit Records | a. Enforce access restrictions using [Assignment: organization-defined automated mechanisms]; andb. Automatically generate audit records of the enforcement actions. | Functional | Equal | Automated Access Enforcement / Auditing | CHG-04.1 | Mechanisms exist to perform after-the-fact reviews of configuration change logs to discover any unauthorized changes. | 10 | |
| CM-06(01) | Configuration Settings \| Automated Management, Application, and Verification | Manage, apply, and verify configuration settings for [Assignment: organization-defined system components] using [Assignment: organization-defined automated mechanisms]. | Functional | Intersects With | Automated Central Management & Verification | CFG-02.2 | Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar | 5 | |
| CM-06(02) | Configuration Settings \| Respond to Unauthorized Changes | Take the following actions in response to unauthorized changes to [Assignment: organization-defined configuration settings]: [Assignment: organization-defined actions]. | Functional | Equal | Respond To Unauthorized Changes | CFG-02.8 | Mechanisms exist to respond to unauthorized changes to configuration settings as security incidents. | 10 | |
| CM-08(02) | System Component Inventory \| Automated Maintenance | Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [Assignment: organization-defined automated mechanisms]. | Functional | Equal | Configuration Management Database (CMDB) | AST-02.9 | Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information. | 10 | |
| CM-08(04) | System Component Inventory \| Accountability Information | Include in the system component inventory information, a means for identifying by [Selection (one or more): name; position; role], individuals responsible and accountable for administering those components. | Functional | Equal | Accountability Information | AST-03.1 | Mechanisms exist to include capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory | 10 | |
| CP-02(02) | Contingency Plan \| Capacity Planning | Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations. | Functional | Equal | Capacity Planning | CAP-03 | Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations. | 10 | |
| 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-03(01) | Contingency Training \| Simulated Events | Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations. | Functional | Equal | Simulated Events | BCD-03.1 | Mechanisms exist to incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations. | 10 | |
| CP-04(02) | Contingency Plan Testing \| Alternate Processing Site | Test the contingency plan at the alternate processing site:a. To familiarize contingency personnel with the facility and available resources; andb. To evaluate the capabilities of the alternate processing site to support contingency operations. | Functional | Equal | Alternate Storage & Processing Sites | BCD-04.2 | Mechanisms exist to test contingency plans at alternate storage & processing sites to both familiarize contingency personnel with the facility and evaluate the capabilities of the alternate processing site to support contingency operations. | 10 | |
| CP-06(02) | Alternate Storage Site \| Recovery Time and Recovery Point Objectives | Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives. | Functional | Intersects With | Recovery Time / Point Objectives (RTO / RPO) | BCD-01.4 | Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). | 5 | |
| CP-07(04) | Alternate Processing Site \| Preparation for Use | Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions. | Functional | Equal | Preparation for Use | BCD-09.4 | Mechanisms exist to prepare the alternate processing alternate to support essential missions and business functions so that the alternate site is capable of being used as the primary site. | 10 | |
| 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-08(04) | Telecommunications Services \| Provider Contingency Plan | a. Require primary and alternate telecommunications service providers to have contingency plans;b. Review provider contingency plans to ensure that the plans meet organizational contingency requirements; andc. Obtain evidence of contingency testing and training by providers [Assignment: organization-defined frequency]. | Functional | Equal | Provider Contingency Plan | BCD-10.3 | Mechanisms exist to contractually-require external service providers to have contingency plans that meet organizational contingency requirements. | 10 | |
| CP-09(02) | System Backup \| Test Restoration Using Sampling | Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing. | Functional | Equal | Test Restoration Using Sampling | BCD-11.5 | Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing. | 10 | |
| CP-09(03) | System Backup \| Separate Storage for Critical Information | Store backup copies of [Assignment: organization-defined critical system software and other security-related information] in a separate facility or in a fire rated container that is not collocated with the operational system. | Functional | Equal | Separate Storage for Critical Information | BCD-11.2 | Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up. | 10 | |
| CP-09(05) | System Backup \| Transfer to Alternate Storage Site | Transfer system backup information to the alternate storage site [Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives]. | Functional | Equal | Transfer to Alternate Storage Site | BCD-11.6 | Mechanisms exist to transfer backup data to the alternate storage site at a rate that is capable of meeting both Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). | 10 | |

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationsh | Notes |
|---|---|---|---|---|---|---|---|---|---|
| CP-10(04) | System Recovery and Reconstitution \| Restore Within Time Period | Provide the capability to restore system components within [Assignment: organization-defined restoration time periods] from configuration-controlled and integrity-protected information representing a known, operational state for the components. | Functional | Equal | Restore Within Time Period | BCD-12.4 | Mechanisms exist to restore Technology Assets, Applications, Services and/or Data (TAASD) within organization-defined restoration time-periods from configuration-controlled and integrity-protected information; representing a known, | 10 | |
| IA-02(05) | Identification and Authentication (organizational Users) \| Individual Authentication with Group Authentication | When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources. | Functional | Equal | Group Authentication | IAC-02.1 | Mechanisms exist to require individuals to be authenticated with an individual authenticator when a group authenticator is utilized. | 10 | |
| IA-12(04) | Identity Proofing \| In-person Validation and Verification | Require that the validation and verification of identity evidence be conducted in person before a designated registration authority. | Functional | Intersects With | User Provisioning & De-Provisioning | IAC-07 | Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights. | 5 | |
| IA-12(04) | Identity Proofing \| In-person Validation and Verification | Require that the validation and verification of identity evidence be conducted in person before a designated registration authority. | Functional | Intersects With | In-Person or Trusted Third-Party Registration | IAC-10.3 | Mechanisms exist to conduct in-person or trusted third-party identify verification before user accounts for third-parties are created. | 5 | |
| IA-12(04) | Identity Proofing \| In-person Validation and Verification | Require that the validation and verification of identity evidence be conducted in person before a designated registration authority. | Functional | Intersects With | In-Person Validation & Verification | IAC-28.4 | Mechanisms exist to require that the validation and verification of identity evidence be conducted in person before a designated registration authority. | 5 | |
| IR-02(01) | Incident Response Training \| Simulated Events | Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations. | Functional | Equal | Simulated Incidents | IRO-05.1 | Mechanisms exist to incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations. | 10 | |
| IR-02(02) | Incident Response Training \| Automated Training Environments | Provide an incident response training environment using [Assignment: organization-defined automated mechanisms]. | Functional | Equal | Automated Incident Response Training Environments | IRO-05.2 | Automated mechanisms exist to provide a more thorough and realistic incident response training environment. | 10 | |
| 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(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-05(01) | Incident Monitoring \| Automated Tracking, Data Collection, and Analysis | Track incidents and collect and analyze incident information using [Assignment: organization-defined automated mechanisms]. | Functional | Equal | Automated Tracking, Data Collection & Analysis | IRO-09.1 | Automated mechanisms exist to assist in the tracking, collection and analysis of information from actual and potential cybersecurity and data protection incidents. | 10 | |
| MA-02(02) | Controlled Maintenance \| Automated Maintenance Activities | a. Schedule, conduct, and document maintenance, repair, and replacement actions for the system using [Assignment: organization-defined automated mechanisms]; andb. Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed. | Functional | Equal | Automated Maintenance Activities | MNT-02.1 | Automated mechanisms exist to schedule, conduct and document maintenance and repairs. | 10 | |
| MA-04(03) | Nonlocal Maintenance \| Comparable Security and Sanitization | a. Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; orb. Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system. | Functional | Equal | Remote Maintenance Comparable Security & Sanitization | MNT-05.6 | Mechanisms exist to require Technology Assets, Applications and/or Services (TAAS) performing remote, non-local maintenance and/or diagnostic services implement a security capability comparable to the capability implemented on the system being serviced. | 10 | |
| MA-05(01) | Maintenance Personnel \| Individuals Without Appropriate Access | a. Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; and2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; andb. Develop and implement [Assignment: organization-defined alternate controls] in the event a system component cannot be sanitized, removed, or disconnected from the system. | Functional | Intersects With | Maintenance Personnel Without Appropriate Access | MNT-06.1 | Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated. | 5 | |
| MP-06(01) | Media Sanitization \| Review, Approve, Track, Document, and Verify | Review, approve, track, document, and verify media sanitization and disposal actions. | Functional | Equal | System Media Sanitization Documentation | DCH-09.1 | Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions. | 10 | |
| MP-06(02) | Media Sanitization \| Equipment Testing | Test sanitization equipment and procedures [Assignment: organization-defined frequency] to ensure that the intended sanitization is being achieved. | Functional | Equal | Equipment Testing | DCH-09.2 | Mechanisms exist to test sanitization equipment and procedures to verify that the intended result is achieved. | 10 | |
| MP-06(03) | Media Sanitization \| Nondestructive Techniques | portable storage devices prior to connecting such devices to the system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable | Functional | Intersects With | First Time Use Sanitization | DCH-09.4 | Mechanisms exist to apply nondestructive sanitization techniques to portable storage devices prior to first use. | 5 | |
| MP-06(03) | Media Sanitization \| Nondestructive Techniques | Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices]. | Functional | Intersects With | System Media Sanitization | DCH-09 | Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse. | 5 | |
| MP-06(03) | Media Sanitization \| Nondestructive Techniques | Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable | Functional | Intersects With | Sanitization of Personal Data (PD) | DCH-09.3 | Mechanisms exist to facilitate the sanitization of Personal Data (PD). | 5 | |
| PE-03(01) | Physical Access Control \| System Access | Enforce physical access authorizations to the system in addition to the physical access controls for the facility at [Assignment: organization-defined physical spaces containing one or more components of the system]. | Functional | Equal | Access To Critical Systems | PES-03.4 | Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulated data, in addition to the physical access controls for the facility. | 10 | |

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationsh | Notes |
|---|---|---|---|---|---|---|---|---|---|
| PE-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-08(01) | Visitor Access Records \| Automated Records Maintenance and Review | Maintain and review visitor access records using [Assignment: organization-defined automated mechanisms]. | Functional | Equal | Automated Records Management & Review | PES-06.4 | Automated mechanisms exist to facilitate the maintenance and review of visitor access records. | 10 | |
| 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-13(02) | Fire Protection \| Suppression Systems — Automatic Activation and Notification | a. Employ fire suppression systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders]; andb. Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis. | Functional | Intersects With | Automatic Fire Suppression | PES-08.3 | Facility security mechanisms exist to employ an automatic fire suppression capability for critical systems when the facility is not staffed on a continuous basis. | 5 | |
| PE-13(02) | Fire Protection \| Suppression Systems — Automatic Activation and Notification | a. Employ fire suppression systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders]; andb. Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis. | Functional | Intersects With | Fire Suppression Devices | PES-08.2 | Facility security mechanisms exist to utilize fire suppression devices/systems that provide automatic notification of any activation to organizational personnel and emergency responders. | 5 | |
| PE-15(01) | Water Damage Protection \| Automation Support | Detect the presence of water near the system and alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms]. | Functional | Equal | Automation Support for Water Damage Protection | PES-07.6 | Facility security mechanisms exist to detect the presence of water in the vicinity of critical systems and alert facility maintenance and IT personnel. | 10 | |
| PE-18 | Location of System Components | Position system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access. | Functional | Intersects With | Equipment Siting & Protection | PES-12 | Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. | 5 | |
| PS-04(02) | Personnel Termination \| Automated Actions | Use [Assignment: organization-defined automated mechanisms] to [Selection (one or more): notify [Assignment: organization-defined personnel or roles] of individual termination actions; disable access to system resources]. | Functional | Equal | Automated Employment Status Notifications | HRS-09.4 | Mechanisms exist to notify Identity and Access Management (IAM) personnel or roles upon termination of an individual employment or | 10 | |
| 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 | |
| SA-04(05) | Acquisition Process \| System, Component, and Service Configurations | Require the developer of the system, system component, or system service to:a. Deliver the system, component, or service with [Assignment: organization-defined security configurations] implemented; andb. Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade. | Functional | Equal | Pre-Established Secure Configurations | TDA-02.4 | Mechanisms exist to ensure vendors / manufacturers:<br>(1) Deliver the Technology Asset, Application and/or Service (TAAS) with a pre-established, secure configuration implemented; and<br>(2) Use the pre-established, secure configuration as the default for any subsequent TAAS reinstallation or upgrade. | 10 | |
| SA-16 | Developer-provided Training | Require the developer of the system, system component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: [Assignment: organization-defined training]. | Functional | Equal | Developer-Provided Training | TDA-16 | Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to provide training on the correct use and operation of the Technology Asset, Application and/or Service (TAAS). | 10 | |
| SA-17 | Developer Security and Privacy Architecture and Design | Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that:a. Is consistent with the organization's security and privacy architecture that is an integral part the organization's enterprise architecture;b. Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; andc. Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection. | Functional | Equal | Developer Architecture & Design | TDA-05 | Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a design specification and security architecture that:<br>(1) Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture;<br>(2) Accurately and completely describes the required security functionality and the allocation of security, compliance and resilience controls among physical and logical components; and<br>(3) Expresses how individual security functions, mechanisms and services work together to provide required security | 10 | |
| SA-21 | Developer Screening | Require that the developer of [Assignment: organization-defined system, system component, or system service]:a. Has appropriate access authorizations as determined by assigned [Assignment: organization-defined official government duties]; andb. Satisfies the following additional personnel screening criteria: [Assignment: organization-defined additional personnel screening criteria]. | Functional | Equal | Developer Screening | TDA-13 | Mechanisms exist to ensure that the developers of Technology Assets, Applications and/or Services (TAAS) have the requisite skillset and appropriate access authorizations. | 10 | |
| 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-07(18) | Boundary Protection \| Fail Secure | Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device. | Functional | Intersects With | Secure Engineering Principles | SEA-01 | Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or | 5 | |
| 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-12(01) | Cryptographic Key Establishment and Management \| Availability | Maintain availability of information in the event of the loss of cryptographic keys by users. | Functional | Equal | Cryptographic Key Loss or Change | CRY-09.3 | Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users. | 10 | |

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationsh | Notes |
|---|---|---|---|---|---|---|---|---|---|
| SC-24 | Fail in Known State | Fail to a [Assignment: organization-defined known system state] for the following failures on the indicated components while preserving [Assignment: organization-defined system state information] in failure: [Assignment: list of organization-defined types of system failures on organization-defined system components]. | Functional | Intersects With | Fail Secure | SEA-07.2 | Mechanisms exist to enable systems to fail to an organization-defined known-state for types of failures, preserving system state information in failure. | 5 | |
| 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(12) | System Monitoring \| Automated Organization-generated Alerts | Alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [Assignment: organization-defined activities that trigger alerts]. | Functional | Intersects With | Automated Alerts | MON-01.12 | Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications. | 5 | |
| SI-04(12) | System Monitoring \| Automated Organization-generated Alerts | Alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [Assignment: organization-defined activities that trigger alerts]. | Functional | Intersects With | Real-Time Alerts of Event Logging Failure | MON-05.1 | Mechanisms exist to provide 24x7x365 near real-time alerting capability when an event log processing failure occurs. | 5 | |
| SI-04(14) | System Monitoring \| Wireless Intrusion Detection | Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system. | Functional | Intersects With | Wireless Network Monitoring | MON-01.5 | Mechanisms exist to monitor wireless network segments for: (1) Rogue wireless devices; and (2) Anomalous and/or hostile activities. | 5 | |
| SI-04(20) | System Monitoring \| Privileged Users | Implement the following additional monitoring of privileged users: [Assignment: organization-defined additional monitoring]. | Functional | Equal | Privileged User Oversight | MON-01.15 | Mechanisms exist to implement enhanced activity monitoring for privileged users. | 10 | |
| SI-04(22) | System Monitoring \| Unauthorized Network Services | a. Detect network services that have not been authorized or approved by [Assignment: organization-defined authorization or approval processes]; andb. [Selection (one or more): Audit; Alert [Assignment: organization-defined personnel or roles]] when detected. | Functional | Equal | Unauthorized Network Services | MON-11.2 | Automated mechanisms exist to detect unauthorized network services and alert incident response personnel. | 10 | |
| SI-05(01) | Security Alerts, Advisories, and Directives \| Automated Alerts and Advisories | Broadcast security alert and advisory information throughout the organization using [Assignment: organization-defined automated mechanisms]. | Functional | Intersects With | Threat Intelligence Feeds | THR-03 | Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls. | 5 | |
| SI-06 | Security and Privacy Function Verification | a. Verify the correct operation of [Assignment: organization-defined security and privacy functions];b. Perform the verification of the functions specified in SI-06a [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]];c. Alert [Assignment: organization-defined personnel or roles] to failed security and privacy verification tests; andd. [Selection (one or more): Shut the system down; Restart the system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered. | Functional | Intersects With | Control Functionality Verification | CHG-06 | Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed. | 5 | |
| SI-07(02) | Software, Firmware, and Information Integrity \| Automated Notifications of Integrity Violations | Employ automated tools that provide notification to [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification. | Functional | Equal | Automated Notifications of Integrity Violations | END-06.3 | Automated mechanisms exist to alert incident response personnel upon discovering discrepancies during integrity verification. | 10 | |
| 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(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 | |
| SR-09 | Tamper Resistance and Detection | Implement a tamper protection program for the system, system component, or system service. | Functional | Intersects With | Logical Tampering Protection | AST-15 | Mechanisms exist to assess the integrity of critical Technology Assets, Applications and/or Services (TAAS) to detect evidence of tampering, where: (1) Logical assessments evaluate the integrity of critical components (e.g., configuration settings); and (2) Physical assessments evaluate assets for evidence of unauthorized access and/or | 5 | |
| SR-09(01) | Tamper Resistance and Detection \| Multiple Stages of System Development Life Cycle | Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle. | Functional | Intersects With | Logical Tampering Protection | AST-15 | Mechanisms exist to assess the integrity of critical Technology Assets, Applications and/or Services (TAAS) to detect evidence of tampering, where: (1) Logical assessments evaluate the integrity of critical components (e.g., configuration settings); and (2) Physical assessments evaluate assets for evidence of unauthorized access and/or | 5 | |