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

Focal Document: **Texas Risk & Authorization Management Program 2.0 - Level 2**
Focal Document URL: https://dir.texas.gov/resource-library-item/tx-ramp-control-baselines-20
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-state-tx-txramp-2-0-level-2.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
AC-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	AC-1 (c)(1) [least every three (3) years] and [following significant changes] AC-1 (c)(2) [at least annually] and [following significant changes]
AC-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	AC-1 (c)(1) [least every three (3) years] and [following significant changes] AC-1 (c)(2) [at least annually] and [following significant changes]
AC-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	AC-1 (c)(1) [least every three (3) years] and [following significant changes] AC-1 (c)(2) [at least annually] and [following significant changes]
AC-02	Account Management	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	5	AC-2 (j) [at least annually]
AC-02	Account Management	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	AC-2 (j) [at least annually]
AC-02	Account Management	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	AC-2 (j) [at least annually]
AC-02	Account Management	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	AC-2 (j) [at least annually]
AC-02 (03)	Account Management | Disable Accounts	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	10	AC-2 (3) (d) [180 days for user accounts]
AC-02 (05)	Account Management | Inactivity Logout	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Session Lock	IAC-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods.	10	AC-2(5) [shorter timeframe than AC-12]
AC-02 (07)	Account Management | Privileged User Accounts	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	10	
AC-02 (09)	Account Management | Restrictions on Use of Shared and Group Accounts	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Restrictions on Shared Groups / Accounts	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	10	
AC-02 (12)	Account Management | Account Monitoring for Atypical Usage	See FD for details. FD = NIST SP 800-53.	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-2 (12)(a) and AC-2 (12)(b) Required for privileged accounts.
AC-03	Access Enforcement	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
AC-03	Access Enforcement	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	
AC-03	Access Enforcement	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
AC-04	Information Flow Enforcement	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	10	
AC-05	Separation of Duties	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Dual Authorization for Change	CHG-04.3	Mechanisms exist to enforce a two-person rule for implementing changes to critical Technology Assets, Applications and/or Services (TAAS).	5	
AC-06	Least Privilege	See FD for details. FD = NIST SP 800-53.	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	See FD for details. FD = NIST SP 800-53.	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	See FD for details. FD = NIST SP 800-53.	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	See FD for details. FD = NIST SP 800-53.	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-6(2) [all security-relevant functions]
AC-06 (05)	Least Privilege | Privileged Accounts	See FD for details. FD = NIST SP 800-53.	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	
AC-06 (07)	Least Privilege | Review of User Privileges	See FD for details. FD = NIST SP 800-53.	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 (09)	Least Privilege | Log Use of Privileged Functions	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Auditing Use of Privileged Functions	IAC-21.4	Mechanisms exist to audit the execution of privileged functions.	10	
AC-06 (10)	Least Privilege | Prohibit Non-privileged Users from Executing Privileged Functions	See FD for details. FD = NIST SP 800-53.	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	Unsuccessful Logon Attempts	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Account Lockout	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	10	AC-7(a) [no more than 5] [15 minute]
AC-11	Device Lock	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Session Lock	IAC-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods.	5	AC-11(a) [30 minutes]
AC-12	Session Termination	See FD for details. FD = NIST SP 800-53.	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-14	Permitted Actions Without Identification or Authentication	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Permitted Actions Without Identification or Authorization	IAC-26	Mechanisms exist to identify and document the supporting rationale for specific user actions that can be performed on a system without identification or authentication.	10	
AC-17	Remote Access	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
AC-17 (01)	Remote Access | Monitoring and Control	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Automated Monitoring & Control	NET-14.1	Automated mechanisms exist to monitor and control remote access sessions.	10	
AC-17 (02)	Remote Access | Protection of Confidentiality and Integrity Using Encryption	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Protection of Confidentiality / Integrity Using Encryption	NET-14.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).	10	
AC-17 (03)	Remote Access | Managed Access Control Points	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Managed Access Control Points	NET-14.3	Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).	10	
AC-17 (04)	Remote Access | Privileged Commands and Access	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Remote Privileged Commands & Sensitive Data Access	NET-14.4	Mechanisms exist to restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.	10	
AC-17 (09)	Remote Access | Disconnect or Disable Access	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Expeditious Disconnect / Disable Capability	NET-14.8	Mechanisms exist to provide the capability to expeditiously disconnect or disable a user's remote access session.	10	AC-17(9) [15 minutes]
AC-18	Wireless Access	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
AC-18	Wireless Access	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
AC-19	Access Control for Mobile Devices	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Access Control For Mobile Devices	MDM-02	Mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	10	
AC-19 (05)	Access Control for Mobile Devices | Full Device or Container-based Encryption	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Full Device & Container-Based Encryption	MDM-03	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.	10	AC-5-2 [mobile devices that process/store confidential state data]
AC-20	Use of External Systems	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Use of External Technology Assets, Applications and/or Services (TAAS)	DCH-13	Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.	10	
AC-20 (01)	Use of External Systems | Limits on Authorized Use	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Limits of Authorized Use	DCH-13.1	Mechanisms exist to prohibit external parties, including Technology Assets, Applications and/or Services (TAAS), from storing, processing and transmitting data unless authorized individuals first:(1) Verifying the implementation of required security, compliance and/or resilience controls; or(2) Retaining a processing agreement with the entity hosting the external TAAS.	10	
AC-22	Publicly Accessible Content	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	10	AC-22(d) [at least quarterly]
AT-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	AT-1 (c)(1) [least every three (3) years] and [following significant changes] AT-1 (c)(2) [at least annually] and [following significant changes]
AT-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	AT-1 (c)(1) [least every three (3) years] and [following significant changes] AT-1 (c)(2) [at least annually] and [following significant changes]
AT-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	AT-1 (c)(1) [least every three (3) years] and [following significant changes] AT-1 (c)(2) [at least annually] and [following significant changes]

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
AT-02	Literacy Training and Awareness	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	10	AT-02 (a)(1) [at least annually]
AT-02 (02)	Literacy Training and Awareness | Insider Threat	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Insider Threat Awareness	THR-05	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.	10	
AT-02 (03)	Literacy Training and Awareness | Social Engineering and Mining	See FD for details. FD = NIST SP 800-53.	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 mining.	10	
AT-03	Role-based Training	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.	5	AT-3(a)(1) [at least annually]
AT-04	Training Records	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Security, Compliance & Resilience Training Records	SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including:(1) Initial security, compliance and resilience awareness training;(2) Recurring awareness training; and(3) Technology Assets, Applications and/or Services (TAAS)-specific training.	10	AT-4(b) [at least 1 year]
AU-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	AU-1 (c)(1) [least every three (3) years] and [following significant changes] AU-1 (c)(2) [at least annually] and [following significant changes]
AU-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	AU-1 (c)(1) [least every three (3) years] and [following significant changes] AU-1 (c)(2) [at least annually] and [following significant changes]
AU-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	AU-1 (c)(1) [least every three (3) years] and [following significant changes] AU-1 (c)(2) [at least annually] and [following significant changes]
AU-02	Event Logging	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	AU-2 (a) [Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes]
AU-02	Event Logging	See FD for details. FD = NIST SP 800-53.	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-2 (a) [Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes]
AU-03	Content of Audit Records	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:(1) Establish what type of event occurred;(2) When (date and time) the event occurred;(3) Where the event occurred;(4) The source of the event;(5) The outcome (success or failure) of the event; and(6) The identity of any user/subject associated with the event.	10	
AU-03 (01)	Content of Audit Records | Additional Audit Information	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Sensitive Event Log Information	MON-03.1	Mechanisms exist to protect sensitive/regulated data contained in log files.	5	AU-3 (1) [Assignment: organization-defined additional, more detailed information] [session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon]
AU-04	Audit Log Storage Capacity	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Event Log Storage Capacity	MON-04	Mechanisms exist to allocate and proactively manage sufficient event log storage capacity to reduce the likelihood of such capacity being exceeded.	10	
AU-05	Response to Audit Logging Process Failures	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Response To Event Log Processing Failures	MON-05	Mechanisms exist to alert appropriate personnel in the event of a log processing failure and take actions to remedy the disruption.	10	
AU-06	Audit Record Review, Analysis, and Reporting	See FD for details. FD = NIST SP 800-53.	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-6(a) [at least monthly]
AU-06	Audit Record Review, Analysis, and Reporting	See FD for details. FD = NIST SP 800-53.	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-6(a) [at least monthly]
AU-08	Time Stamps	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	5	
AU-09	Protection of Audit Information	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Time Stamps	MON-07	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to use an authoritative time source to generate time stamps for event logs.	5	
AU-09	Protection of Audit Information	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	10	
AU-11	Audit Record Retention	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	10	AU-11 [at least 60 days]
AU-12	Audit Record Generation	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	5	
CA-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	CA-1 (c)(1) [least every three (3) years] and [following significant changes] CA-1 (c)(2) [at least annually] and [following significant changes]
CA-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	CA-1 (c)(1) [least every three (3) years] and [following significant changes] CA-1 (c)(2) [at least annually] and [following significant changes]
CA-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	CA-1 (c)(1) [least every three (3) years] and [following significant changes] CA-1 (c)(2) [at least annually] and [following significant changes]
CA-02	Control Assessments	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	CA-2(d) [at least annually]
CA-02	Control Assessments	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	5	CA-2(d) [at least annually]
CA-02	Control Assessments	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	CA-2(d) [at least annually]
CA-02	Control Assessments	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	CA-2(d) [at least annually]
CA-02	Control Assessments	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	CA-2(d) [at least annually]
CA-03	Information Exchange	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection:(1) Interface characteristics;(2) Security, compliance and resilience requirements; and;(3) The nature of the information communicated.	5	CA-3(c) [at least annually]
CA-05	Plan of Action and Milestones	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency(ies);(4) Risk associated with the deficiency(ies);(5) Source deficiency identification/detection;(6) Temporary compensating controls, if applicable;(7) Point of Contact (POC) (e.g., asset/process owner);(8) Resources required to conduct remediation actions;(9) Planned remedial actions to the	5	CA-5(b) [at least quarterly]

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
CA-06	Authorization	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	10	CA-6(e) [at least every three years or when a significant change occurs]
CA-07	Continuous Monitoring	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
CA-07 (04)	Continuous Monitoring | Risk Monitoring	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Risk Monitoring	RSK-11	Mechanisms exist to ensure risk monitoring as an integral part of the continuous monitoring strategy that includes monitoring the effectiveness of security, compliance and resilience controls, compliance and change management.	10	
CA-08	Penetration Testing	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	10	CA-8 [at least annually] CA-8 [for applications that process any confidential state data]
CA-09	Internal System Connections	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Internal System Connections	NET-05.2	Mechanisms exist to control internal system connections through authorizing internal connections of systems and documenting, for each internal connection, the interface characteristics, security requirements and the nature of the information communicated.	10	
CM-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	CM-1 (c)(1) [least every three (3) years] and [following significant changes] CM-1 (c)(2) [at least annually] and [following significant changes]
CM-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	CM-1 (c)(1) [least every three (3) years] and [following significant changes] CM-1 (c)(2) [at least annually] and [following significant changes]
CM-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	CM-1 (c)(1) [least every three (3) years] and [following significant changes] CM-1 (c)(2) [at least annually] and [following significant changes]
CM-02	Baseline Configuration	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations:(1) At least annually;(2) When required due to so; or(3) As part of system component installations and upgrades.	5	
CM-02	Baseline Configuration	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
CM-02 (03)	Baseline Configuration | Retention of Previous Configurations	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Retention Of Previous Configurations	CFG-02.3	Mechanisms exist to retain previous versions of baseline configuration to support roll back.	10	
CM-03	Configuration Change Control	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
CM-03	Configuration Change Control	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
CM-03 (02)	Configuration Change Control | Testing, Validation, and Documentation of Changes	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	5	
CM-03 (02)	Configuration Change Control | Testing, Validation, and Documentation of Changes	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	5	
CM-03 (04)	Configuration Change Control | Security and Privacy Representatives	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Security, Compliance & Resilience Representative for Asset Lifecycle Changes	CHG-02.3	Mechanisms exist to include a cybersecurity and/or data protection representative in the configuration change control review process.	10	
CM-04	Impact Analyses	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	10	
CM-04 (02)	Impact Analyses | Verification of Controls	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	10	
CM-05	Access Restrictions for Change	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Governing Access Restriction for Change	END-03.2	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to Technology Assets, Applications and/or Services (TAAS).	5	
CM-05	Access Restrictions for Change	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
CM-05 (05)	Access Restrictions for Change | Privilege Limitation for Production and Operation	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Permissions To Implement Changes	CHG-04.4	Mechanisms exist to limit operational privileges for implementing changes.	10	CM-5(5) [at least quarterly]
CM-06	Configuration Settings	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
CM-06	Configuration Settings	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	5	
CM-07	Least Functionality	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	10	
CM-07 (01)	Least Functionality | Periodic Review	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	10	CM-7(1)(a) [at least quarterly]
CM-07 (02)	Least Functionality | Prevent Program Execution	See FD for details. FD = NIST SP 800-53.	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	See FD for details. FD = NIST SP 800-53.	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 (05)	Least Functionality | Authorized Software	See FD for details. FD = NIST SP 800-53.	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-7(5) (c) [at least annually or when there is a change]
CM-08	System Component Inventory	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:(1) Accurately reflects the current TAASD in use;(2) Identifies authorized software products, including business justification details;(3) Is at the level of granularity deemed necessary for tracking and reporting;(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and(5) Is available for review and audit by designated organizational personnel.	5	CM-8(b) [at least quarterly]
CM-08	System Component Inventory	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Component Duplication Avoidance	AST-02.3	Mechanisms exist to establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components that prevents assets from being duplicated in other asset inventories.	5	CM-8(b) [at least quarterly]
CM-08 (01)	System Component Inventory | Updates During Installation and Removal	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Updates During Installations / Removals	AST-02.1	Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades.	10	
CM-09	Configuration Management Plan	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
CM-09	Configuration Management Plan	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5	
CM-10	Software Usage Restrictions	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Software Usage Restrictions	CFG-04	Mechanisms exist to enforce software usage restrictions to comply with applicable contract agreements and copyright laws.	10	
CM-11	User-installed Software	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	5	CM-11(c) [at least monthly]
CM-11	User-installed Software	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5	CM-11(c) [at least monthly]
CM-12	Information Location	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Information Location	DCH-24	Mechanisms exist to identify and document the location of information and the specific system components on which the information resides.	10	
CP-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	CP-1 (c)(1) [least every three (3) years] and [following significant changes] CP-1 (c)(2) [at least annually] and [following significant changes]
CP-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	CP-1 (c)(1) [least every three (3) years] and [following significant changes] CP-1 (c)(2) [at least annually] and [following significant changes]
CP-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	CP-1 (c)(1) [least every three (3) years] and [following significant changes] CP-1 (c)(2) [at least annually] and [following significant changes]
CP-02	Contingency Plan	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	CP-2(d) [at least annually]
CP-02	Contingency Plan	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Ongoing Contingency Planning	BCD-06	Mechanisms exist to update contingency plans due to changes affecting:(1) People (e.g., personnel changes);(2) Processes (e.g., new, altered or decommissioned business practices, including third-party services)(3) Technology (e.g., [illegible])	5	CP-2(d) [at least annually]
CP-03	Contingency Training	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Contingency Training	BCD-03	Mechanisms exist to adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities.	10	CP-3(a)(1) [14 days] CP-3(a)(3) [at least annually]

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
CP-04	Contingency Plan Testing	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5	CP-4(a) [at least every 2 years] CP-4(a) [tabletop simulation]
CP-04	Contingency Plan Testing	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	CP-4(a) [at least every 2 years] CP-4(a) [tabletop simulation]
CP-06	Alternate Storage Site	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Alternate Storage Site	BCD-08	Mechanisms exist to establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup information.	10	
CP-07	Alternate Processing Site	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Alternate Processing Site	BCD-09	Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.	10	
CP-08	Telecommunications Services	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Telecommunications Services Availability	BCD-10	Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services.	5	
CP-09	System Backup	See FD for details. FD = NIST SP 800-53.	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-9 (a) [daily incremental; weekly full] CP-9 (b) [daily incremental; weekly full]
CP-09 (01)	System Backup | Testing for Reliability and Integrity	See FD for details. FD = NIST SP 800-53.	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-9(1) [at least annually]
CP-09 (08)	System Backup | Cryptographic Protection	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	10	CP-9(3) [confidential state data]
CP-10	System Recovery and Reconstitution	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	5	
CP-10	System Recovery and Reconstitution	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
CP-10	System Recovery and Reconstitution	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
IA-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	IA-1 (c)(1) [least every three (3) years] and [following significant changes] IA-1 (c)(2) [at least annually] and [following significant changes]
IA-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	IA-1 (c)(1) [least every three (3) years] and [following significant changes] IA-1 (c)(2) [at least annually] and [following significant changes]
IA-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	IA-1 (c)(1) [least every three (3) years] and [following significant changes] IA-1 (c)(2) [at least annually] and [following significant changes]
IA-02	Identification and Authentication (organizational Users)	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	10	
IA-02 (01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:(1) Remote network access;(2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or(3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	5	
IA-02 (01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Local Access to Privileged Accounts	IAC-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	5	
IA-02 (01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Information Assurance Enabled Products	TDA-02.2	Mechanisms exist to limit the use of commercially-provided Information Assurance (IA) and IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated or NSA-approved.	5	
IA-02 (01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Out-of-Band Multi-Factor Authentication	IAC-06.4	Mechanisms exist to implement Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.	5	
IA-02 (01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5	
IA-02 (01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Network Access to Non-Privileged Accounts	IAC-06.2	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts.	5	
IA-02 (01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Hardware Token-Based Authentication	IAC-10.7	Automated mechanisms exist to ensure organization-defined token quality requirements are satisfied for hardware token-based authentication.	5	
IA-02 (08)	Identification and Authentication (organizational Users) | Access to Accounts — Replay Resistant	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Replay-Resistant Authentication	IAC-02.2	Automated mechanisms exist to employ replay-resistant authentication.	10	IA-2(8) [privileged accounts]
IA-03	Device Identification and Authentication	See FD for details. FD = NIST SP 800-53.	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-04	Identifier Management	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	IA-4(d) [at least two years]
IA-04	Identifier Management	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).	5	IA-4(d) [at least two years]
IA-04 (04)	Identifier Management | Identify User Status	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	IA-4(4) [to include contractors; foreign nationals; non-organizational users]
IA-04 (04)	Identifier Management | Identify User Status	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	User Identity (ID) Management	IAC-09.1	Mechanisms exist to ensure proper user identification management for non-consumer users and administrators.	5	IA-4(4) [to include contractors; foreign nationals; non-organizational users]
IA-04 (04)	Identifier Management | Identify User Status	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Identity User Status	IAC-09.2	Mechanisms exist to identify contractors and other third-party users through unique username characteristics.	5	IA-4(4) [to include contractors; foreign nationals; non-organizational users]
IA-05	Authenticator Management	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the	5	
IA-05	Authenticator Management	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	
IA-05 (01)	Authenticator Management | Password-based Authentication	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Automated Support For Password Strength	IAC-10.4	Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.	5	IA-5(h) [case sensitive, minimum twelve characters, at least one upper-case, lower-case, letters, numbers, and special characters]
IA-05 (01)	Authenticator Management | Password-based Authentication	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	IA-5(h) [case sensitive, minimum twelve characters, at least one upper-case, lower-case, letters, numbers, and special characters]
IA-05 (01)	Authenticator Management | Password-based Authentication	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to:(1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	IA-5(h) [case sensitive, minimum twelve characters, at least one upper-case, lower-case, letters, numbers, and special characters]
IA-05 (02)	Authenticator Management | Public Key-based Authentication	See FD for details. FD = NIST SP 800-53.	Functional	Equal	PKI-Based Authentication	IAC-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	10	
IA-05 (06)	Authenticator Management | Protection of Authenticators	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	User Responsibilities for Account Management	IAC-18	Mechanisms exist to compel users to follow accepted practices in the use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards, certificates, etc.).	5	
IA-05 (06)	Authenticator Management | Protection of Authenticators	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
IA-05 (07)	Authenticator Management | No Embedded Unencrypted Static Authenticators	See FD for details. FD = NIST SP 800-53.	Functional	Equal	No Embedded Unencrypted Static Authenticators	IAC-10.6	Mechanisms exist to ensure that unencrypted, static authenticators are not embedded in applications, scripts or stored on function keys.	10	
IA-06	Authentication Feedback	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Authenticator Feedback	IAC-11	Mechanisms exist to obscure the feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
IA-07	Cryptographic Module Authentication	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Cryptographic Module Authentication	IAC-12	Mechanisms exist to ensure cryptographic modules adhere to applicable statutory, regulatory and contractual requirements for security strength.	5	
IA-07	Cryptographic Module Authentication	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Automated Authentication Through Cryptographic Modules	CRY-02	Automated mechanisms exist to enable systems to authenticate to a cryptographic module.	5	
IA-08	Identification and Authentication (non-organizational Users)	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Identification & Authentication for Non-Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	10	
IA-11	Re-authentication	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Re-Authentication	IAC-14	Mechanisms exist to force users and devices to re-authenticate according to organization-defined circumstances that necessitate re-authentication.	10	
IR-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	IR-1 (c)(1) [least every three (3) years] and [following significant changes] IR-1 (c)(2) [at least annually] and [following significant changes]
IR-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	IR-1 (c)(1) [least every three (3) years] and [following significant changes] IR-1 (c)(2) [at least annually] and [following significant changes]
IR-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	5	IR-1 (c)(1) [least every three (3) years] and [following significant changes] IR-1 (c)(2) [at least annually] and [following significant changes]
IR-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	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-1 (c)(1) [least every three (3) years] and [following significant changes] IR-1 (c)(2) [at least annually] and [following significant changes]
IR-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	IR-1 (c)(1) [least every three (3) years] and [following significant changes] IR-1 (c)(2) [at least annually] and [following significant changes]
IR-02	Incident Response Training	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5	IR-2(a)(1) [14 days] IR-2(a)(3) [at least annually]
IR-03	Incident Response Testing	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5	IR-3 [at least annually] [tabletop simulation]
IR-03 (02)	Incident Response Testing | Coordination with Related Plans	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Coordination with Related Plans	IRO-06.1	Mechanisms exist to coordinate incident response testing with organizational elements responsible for related plans.	10	
IR-04	Incident Handling	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
IR-05	Incident Monitoring	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	10	
IR-06	Incident Reporting	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	5	IR-6(a) [within 48 hours of discovery] IR-6(b) [the Texas Department of Information Resources if the incident involves state of Texas confidential information]
IR-06	Incident Reporting	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Regulatory & Law Enforcement Contacts	IRO-14	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.	5	IR-6(a) [within 48 hours of discovery] IR-6(b) [the Texas Department of Information Resources if the incident involves state of Texas confidential information]
IR-06	Incident Reporting	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	5	IR-6(a) [within 48 hours of discovery] IR-6(b) [the Texas Department of Information Resources if the incident involves state of Texas confidential information]
IR-07	Incident Response Assistance	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Incident Reporting Assistance	IRO-11	Mechanisms exist to provide incident response advice and assistance to users of Technology Assets, Applications and/or Services (TAAS) for the handling and reporting of actual and potential cybersecurity and data protection incidents.	10	
IR-08	Incident Response Plan	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	10	IR-8(a)(9) [at least annually]
IR-09	Information Spillage Response	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive/regulated data spills.	5	
IR-09	Information Spillage Response	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Sensitive / Regulated Data Spill Responsible Personnel	IRO-12.1	Mechanisms exist to formally assign personnel or roles with responsibility for responding to sensitive/regulated data spills.	5	
MA-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	10	MA-1 (c)(1) [least every three (3) years] and [following significant changes] MA-1 (c)(2) [at least annually] and [following significant changes]
MA-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Remote Maintenance Notifications	MNT-05.2	Mechanisms exist to require maintenance personnel to notify affected stakeholders when remote, non-local maintenance is planned (e.g., date/time).	5	MA-1 (c)(1) [least every three (3) years] and [following significant changes] MA-1 (c)(2) [at least annually] and [following significant changes]
MA-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	5	MA-1 (c)(1) [least every three (3) years] and [following significant changes] MA-1 (c)(2) [at least annually] and [following significant changes]
MA-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	MA-1 (c)(1) [least every three (3) years] and [following significant changes] MA-1 (c)(2) [at least annually] and [following significant changes]
MA-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	MA-1 (c)(1) [least every three (3) years] and [following significant changes] MA-1 (c)(2) [at least annually] and [following significant changes]
MA-02	Controlled Maintenance	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).	10	MA-2(d) [confidential state data]
MA-03	Maintenance Tools	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	5	MA-3(b) [at least annually]
MA-03 (01)	Maintenance Tools | Inspect Tools	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Inspect Tools	MNT-04.1	Mechanisms exist to inspect maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.	10	
MA-03 (02)	Maintenance Tools | Inspect Media	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Inspect Media	MNT-04.2	Mechanisms exist to check media containing diagnostic and test programs for malicious code before the media are used.	10	
MA-03 (03)	Maintenance Tools | Prevent Unauthorized Removal	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Prevent Unauthorized Removal	MNT-04.3	Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational information.	10	
MA-04	Nonlocal Maintenance	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	5	
MA-04	Nonlocal Maintenance	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Remote Maintenance Notifications	MNT-05.2	Mechanisms exist to require maintenance personnel to notify affected stakeholders when remote, non-local maintenance is planned (e.g., date/time).	5	
MA-04	Nonlocal Maintenance	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	5	
MA-05	Maintenance Personnel	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Authorized Maintenance Personnel	MNT-06	Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.	10	
MA-06	Timely Maintenance	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Timely Maintenance	MNT-03	Mechanisms exist to obtain maintenance support and/or spare parts for Technology Assets, Applications and/or Services (TAAS) within a defined Recovery Time Objective (RTO).	10	
MP-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	MP-1 (c)(1) [least every three (3) years] and [following significant changes] MP-1 (c)(2) [at least annually] and [following significant changes]
MP-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	MP-1 (c)(1) [least every three (3) years] and [following significant changes] MP-1 (c)(2) [at least annually] and [following significant changes]

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
MP-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	MP-1 (c)(1) [least every three (3) years] and [following significant changes] MP-1 (c)(2) [at least annually] and [following significant changes]
MP-02	Media Access	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	5	
MP-02	Media Access	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	5	
MP-03	Media Marking	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
MP-03	Media Marking	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Automated Marking	DCH-04.1	Automated mechanisms exist to mark physical media and digital files to indicate the distribution limitations, handling requirements and applicable security markings (if any) of the information to aid Data Loss Prevention (DLP) technologies.	5	
MP-04	Media Storage	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Media Storage	DCH-06	Mechanisms exist to:(1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and(2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	10	MP-4(a) [all types of digital and non-digital media with confidential state data]
MP-05	Media Transport	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	10	MP-5(a) [all types of digital and non-digital media with confidential state data] [modern encryption standards for digital media; secured in a locked container for non-digital media]
MP-06	Media Sanitization	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
MP-06	Media Sanitization	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
MP-06	Media Sanitization	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).	5	
MP-07	Media Use	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
MP-07	Media Use	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5	
MP-07	Media Use	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Prohibit Use Without Owner	DCH-10.2	Mechanisms exist to prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.	5	
PE-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	PE-1 (c)(1) [least every three (3) years] and [following significant changes] PE-1 (c)(2) [at least annually] and [following significant changes]
PE-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	PE-1 (c)(1) [least every three (3) years] and [following significant changes] PE-1 (c)(2) [at least annually] and [following significant changes]
PE-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	PE-1 (c)(1) [least every three (3) years] and [following significant changes] PE-1 (c)(2) [at least annually] and [following significant changes]
PE-02	Physical Access Authorizations	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	10	PE-2(c) [at least annually]
PE-03	Physical Access Control	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	PE-3(f) [at least annually] PE-3(g) [at least annually]
PE-04	Access Control for Transmission	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	10	
PE-05	Access Control for Output Devices	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Access Control for Output Devices	PES-12.2	Physical security mechanisms exist to restrict access to printers and other system output devices to prevent unauthorized individuals from obtaining the output.	10	
PE-06	Monitoring Physical Access	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	10	PE-6(b) [at least quarterly]
PE-06 (01)	Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	10	
PE-08	Visitor Access Records	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	10	PE-8(a) [at least 1 year] PE-8(b) [at least quarterly]
PE-09	Power Equipment and Cabling	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Supporting Utilities	PES-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	10	
PE-10	Emergency Shutoff	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Emergency Shutoff	PES-07.2	Facility security mechanisms exist to shut off power in emergency situations by:(1) Placing emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel; and(2) Protecting emergency power shutoff capability from unauthorized activation.	10	
PE-11	Emergency Power	See FD for details. FD = NIST SP 800-53.	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-12	Emergency Lighting	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Emergency Lighting	PES-07.4	Facility security mechanisms exist to utilize and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	10	
PE-13	Fire Protection	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Fire Protection	PES-08	Facility security mechanisms exist to utilize and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.	10	
PE-14	Environmental Controls	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Temperature & Humidity Controls	PES-09	Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.	10	
PE-15	Water Damage Protection	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Water Damage Protection	PES-07.5	Facility security mechanisms exist to protect systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly and known to key personnel.	10	
PE-16	Delivery and Removal	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Delivery & Removal	PES-10	Physical security mechanisms exist to isolate information processing facilities from points such as delivery and loading areas and other points to avoid unauthorized access.	10	PE-16(a) [all system components]
PE-17	Alternate Work Site	See FD for details. FD = NIST SP 800-53.	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-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	PL-1 (c)(1) [least every three (3) years] and [following significant changes] PL-1 (c)(2) [at least annually] and [following significant changes]
PL-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	PL-1 (c)(1) [least every three (3) years] and [following significant changes] PL-1 (c)(2) [at least annually] and [following significant changes]
PL-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	PL-1 (c)(1) [least every three (3) years] and [following significant changes] PL-1 (c)(2) [at least annually] and [following significant changes]
PL-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	PL-1 (c)(1) [least every three (3) years] and [following significant changes] PL-1 (c)(2) [at least annually] and [following significant changes]
PL-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	PL-1 (c)(1) [least every three (3) years] and [following significant changes] PL-1 (c)(2) [at least annually] and [following significant changes]
PL-02	System Security and Privacy Plans	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Plan / Coordinate with Other Organizational Entities	IAO-03.1	Mechanisms exist to plan and coordinate Information Assurance Program (IAP) activities with affected stakeholders before conducting such activities in order to reduce the potential impact on operations.	5	PL-2(c) [at least annually]
PL-02	System Security and Privacy Plans	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including	5	PL-2(c) [at least annually]
PL-02	System Security and Privacy Plans	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that:(1) Contain sufficient detail to assess the security of the network's architecture;(2) Reflect the current architecture of the network environment; and(3) Document all sensitive/regulated data flows.	5	PL-2(c) [at least annually]

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
PL-04	Rules of Behavior	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	5	PL-4(c) [at least every 3 years] PL-4(d) [when the rules are revised or updated]
PL-04	Rules of Behavior	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	PL-4(c) [at least every 3 years] PL-4(d) [when the rules are revised or updated]
PL-04	Rules of Behavior	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	5	PL-4(c) [at least every 3 years] PL-4(d) [when the rules are revised or updated]
PL-04 (01)	Rules of Behavior | Social Media and External Site/application Usage Restrictions	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	10	
PL-08	Security and Privacy Architectures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5	PL-8(b) [at least annually]
PS-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	PS-1 (c)(1) [least every three (3) years] and [following significant changes] PS-1 (c)(2) [at least annually] and [following significant changes]
PS-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	PS-1 (c)(1) [least every three (3) years] and [following significant changes] PS-1 (c)(2) [at least annually] and [following significant changes]
PS-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	PS-1 (c)(1) [least every three (3) years] and [following significant changes] PS-1 (c)(2) [at least annually] and [following significant changes]
PS-02	Position Risk Designation	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	PS-2 (c) [at least every three years]
PS-02	Position Risk Designation	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	PS-2 (c) [at least every three years]
PS-03	Personnel Screening	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10	
PS-04	Personnel Termination	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	10	PS-4 (a) [one day]
PS-05	Personnel Transfer	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Personnel Transfer	HRS-08	Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.	10	PS-5(d)-2 [within 5 days following formal transfer action]
PS-06	Access Agreements	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	5	PS-6(b) [at least annually]
PS-06	Access Agreements	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	5	PS-6(b) [at least annually]
PS-07	External Personnel Security	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Third-Party Personnel	HRS-10	Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party security, compliance and/or resilience roles and responsibilities.	10	PS-7(d)-2 [within 1 day]
PS-08	Personnel Sanctions	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	10	
RA-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	RA-1 (c)(1) [least every three (3) years] and [following significant changes] RA-1 (c)(2) [at least annually] and [following significant changes]
RA-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	RA-1 (c)(1) [least every three (3) years] and [following significant changes] RA-1 (c)(2) [at least annually] and [following significant changes]
RA-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	RA-1 (c)(1) [least every three (3) years] and [following significant changes] RA-1 (c)(2) [at least annually] and [following significant changes]
RA-02	Security Categorization	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that:(1) Document the security categorization results (including supporting rationale) in the security plan for systems; and(2) Ensure the security categorization decision is reviewed and approved by the asset owner.	10	
RA-03	Risk Assessment	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	RA-3(f) [at least every 3 years]
RA-03	Risk Assessment	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	RA-3(f) [at least every 3 years]
RA-05	Vulnerability Monitoring and Scanning	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	RA-5 (d) [high and critical severity vulnerabilities mitigated within thirty days from date of discovery; moderate severity vulnerabilities mitigated within ninety days from date of discovery]
RA-05	Vulnerability Monitoring and Scanning	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5	RA-5 (d) [high and critical severity vulnerabilities mitigated within thirty days from date of discovery; moderate severity vulnerabilities mitigated within ninety days from date of discovery]
RA-05 (02)	Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanned	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5	RA-5(2) [prior to a new scan; when new vulnerabilities are identified and reported]
RA-05 (03)	Vulnerability Monitoring and Scanning | Breadth and Depth of Coverage	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Breadth / Depth of Coverage	VPM-06.2	Mechanisms exist to identify the breadth and depth of coverage for vulnerability scanning that define the system components scanned and types of vulnerabilities that are checked for.	10	
RA-05 (05)	Vulnerability Monitoring and Scanning | Privileged Access	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Privileged Access	VPM-06.3	Mechanisms exist to implement privileged access authorization for selected vulnerability scanning activities.	10	RA-5(5) [operating systems; web applications; databases] [system components that process/store confidential state data]
RA-07	Risk Response	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Risk Response	RSK-06.1	Mechanisms exist to ensure proper risk response actions were performed to remediate findings from security, compliance and/or resilience-related:(1) Assessments;(2) Audits; and/or(3) Incidents.	10	
SA-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional						SA-1 (c)(1) [least every three (3) years] and [following significant changes] SA-1 (c)(2) [at least annually] and [following significant changes]
SA-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	SA-1 (c)(1) [least every three (3) years] and [following significant changes] SA-1 (c)(2) [at least annually] and [following significant changes]
SA-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	SA-1 (c)(1) [least every three (3) years] and [following significant changes] SA-1 (c)(2) [at least annually] and [following significant changes]
SA-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	SA-1 (c)(1) [least every three (3) years] and [following significant changes] SA-1 (c)(2) [at least annually] and [following significant changes]
SA-03	System Development Life Cycle	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
SA-03	System Development Life Cycle	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5	
SA-03	System Development Life Cycle	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
SA-04	Acquisition Process	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5	
SA-04	Acquisition Process	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
SA-04	Acquisition Process	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	5	
SA-04	Acquisition Process	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	5	
SA-04 (01)	Acquisition Process | Functional Properties of Controls	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Functional Properties	TDA-04.1	Mechanisms exist to require software developers to provide information describing the functional properties of the security, compliance and resilience controls to be utilized within Technology Assets, Applications and/or Services (TAAS) in sufficient detail to permit analysis and testing of the controls.	5	
SA-04 (01)	Acquisition Process | Functional Properties of Controls	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that:(1) Contain sufficient detail to assess the security of the network's architecture;(2) Reflect the current architecture of the network environment; and(3) Document all sensitive/regulated data flows.	5	
SA-04 (02)	Acquisition Process | Design and Implementation Information for Controls	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that:(1) Contain sufficient detail to assess the security of the network's architecture;(2) Reflect the current architecture of the network environment; and(3) Document all sensitive/regulated data flows.	5	SA-4(2) [to include security relevant external system interfaces and high-level design]
SA-04 (02)	Acquisition Process | Design and Implementation Information for Controls	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Access to Program Source Code	TDA-20	Mechanisms exist to limit privileges to change software resident within software libraries.	5	SA-4(2) [to include security relevant external system interfaces and high-level design]
SA-04 (02)	Acquisition Process | Design and Implementation Information for Controls	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Functional Properties	TDA-04.1	Mechanisms exist to require software developers to provide information describing the functional properties of the security, compliance and resilience controls to be utilized within Technology Assets, Applications and/or Services (TAAS) in sufficient detail to permit analysis and testing of the controls.	5	SA-4(2) [to include security relevant external system interfaces and high-level design]
SA-04 (09)	Acquisition Process | Functions, Ports, Protocols, and Services in Use	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Ports, Protocols & Services In Use	TDA-02.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to identify early in the Secure Development Life Cycle (SDLC), the functions, ports, protocols and services intended for use.	10	
SA-05	System Documentation	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe:(1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and(3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5	
SA-05	System Documentation	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).	5	
SA-08	Security and Privacy Engineering Principles	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
SA-08	Security and Privacy Engineering Principles	See FD for details. FD = NIST SP 800-53.	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 Services (TAAS).	5	
SA-09	External System Services	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	10	SA-9(a) [for external systems that process/store confidential state data, controls commensurate with the protection mechanisms implemented by the cloud service provider]
SA-09 (02)	External System Services | Identification of Functions, Ports, Protocols, and Services	See FD for details. FD = NIST SP 800-53.	Functional	Equal	External Connectivity Requirements - Identification of Ports, Protocols & Services	TPM-04.2	Mechanisms exist to require External Service Providers (ESPs) to identify and document the business need for ports, protocols and other services it requires to operate its Technology Assets, Applications and/or Services (TAAS).	10	SA-9(2) [all external systems where confidential state data resides]
SA-09 (05)	External System Services | Processing, Storage, and Service Location	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	SA-9(5) [information processing, information and data] [agency-approved locations] [agency-defined requirements]
SA-09 (05)	External System Services | Processing, Storage, and Service Location	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5	SA-9(5) [information processing, information and data] [agency-approved locations] [agency-defined requirements]
SA-09 (05)	External System Services | Processing, Storage, and Service Location	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.	5	SA-9(5) [information processing, information and data] [agency-approved locations] [agency-defined requirements]
SA-10	Developer Configuration Management	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Developer Configuration Management	TDA-14	Mechanisms exist to require system developers and integrators to perform configuration management during system design, development, implementation and operation.	10	
SA-10 (01)	Developer Configuration Management | Software and Firmware Integrity Verification	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Software / Firmware Integrity Verification	TDA-14.1	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware components.	10	
SA-11	Developer Testing and Evaluation	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and(3) Document the results.	10	
SA-15	Development Process, Standards, and Tools	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	
SA-22	Unsupported System Components	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	TDA-17	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by:(1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and(2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	5	
SA-22	Unsupported System Components	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Alternate Sources for Continued Support	TDA-17.1	Mechanisms exist to provide in-house support or contract external providers for support with unsupported Technology Assets, Applications and/or Services (TAAS).	5	
SC-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	SC-1 (c)(1) [least every three (3) years] and [following significant changes] SC-1 (c)(2) [at least annually] and [following significant changes]
SC-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	SC-1 (c)(1) [least every three (3) years] and [following significant changes] SC-1 (c)(2) [at least annually] and [following significant changes]
SC-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	SC-1 (c)(1) [least every three (3) years] and [following significant changes] SC-1 (c)(2) [at least annually] and [following significant changes]
SC-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	SC-1 (c)(1) [least every three (3) years] and [following significant changes] SC-1 (c)(2) [at least annually] and [following significant changes]
SC-02	Separation of System and User Functionality	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Application Partitioning	SEA-03.2	Mechanisms exist to separate user functionality from system management functionality.	10	
SC-04	Information in Shared System Resources	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Information In Shared Resources	SEA-05	Mechanisms exist to prevent unauthorized and unintended information transfer via shared system resources.	10	
SC-05	Denial-of-service Protection	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5	
SC-05	Denial-of-service Protection	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	5	
SC-05	Denial-of-service Protection	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	5	
SC-05	Denial-of-service Protection	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	5	
SC-07	Boundary Protection	See FD for details. FD = NIST SP 800-53.	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	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
SC-07 (03)	Boundary Protection | Access Points	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Limit Network Connections	NET-03.1	Mechanisms exist to limit the number of concurrent external network connections to its Technology Assets, Applications and/or Services (TAAS).	10	
SC-07 (04)	Boundary Protection | External Telecommunications Services	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	External Telecommunications Services	NET-03.2	Mechanisms exist to maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface.	5	SC-7(4)(e) [at least annually]
SC-07 (05)	Boundary Protection | Deny by Default — Allow by Exception	See FD for details. FD = NIST SP 800-53.	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-08	Transmission Confidentiality and Integrity	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	SC-8 [confidentiality and integrity]
SC-08	Transmission Confidentiality and Integrity	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	SC-8 [confidentiality and integrity]
SC-08 (01)	Transmission Confidentiality and Integrity | Cryptographic Protection	See FD for details. FD = NIST SP 800-53.	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-8(1) [prevent unauthorized disclosure]
SC-08 (01)	Transmission Confidentiality and Integrity | Cryptographic Protection	See FD for details. FD = NIST SP 800-53.	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-8(1) [prevent unauthorized disclosure]
SC-08 (01)	Transmission Confidentiality and Integrity | Cryptographic Protection	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	SC-8(1) [prevent unauthorized disclosure]
SC-10	Network Disconnect	See FD for details. FD = NIST SP 800-53.	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-12	Cryptographic Key Establishment and Management	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	5	
SC-13	Cryptographic Protection	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	SC-13(a) [to include encryption for confidential state data] [modern encryption standards]
SC-13	Cryptographic Protection	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Export-Controlled Cryptography	CRY-01.2	Mechanisms exist to address the exporting of cryptographic technologies in compliance with relevant statutory and regulatory requirements.	5	SC-13(a) [to include encryption for confidential state data] [modern encryption standards]
SC-13	Cryptographic Protection	See FD for details. FD = NIST SP 800-53.	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-13(a) [to include encryption for confidential state data] [modern encryption standards]
SC-15	Collaborative Computing Devices and Applications	See FD for details. FD = NIST SP 800-53.	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-17	Public Key Infrastructure Certificates	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	5	
SC-18	Mobile Code	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
SC-20	Secure Name/address Resolution Service (authoritative Source)	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Domain Name Service (DNS) Resolution	NET-10	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5	
SC-21	Secure Name/address Resolution Service (recursive or Caching Resolver)	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	NET-10.2	Mechanisms exist to perform data origin authentication and data integrity verification on the Domain Name Service (DNS) resolution responses received from authoritative sources when requested by client systems.	10	
SC-22	Architecture and Provisioning for Name/address Resolution Service	See FD for details. FD = NIST SP 800-53.	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	Session Authenticity	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Session Integrity	NET-09	Mechanisms exist to protect the authenticity and integrity of communications sessions.	10	
SC-28	Protection of Information at Rest	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	SC-28 [confidentiality and integrity] [confidential state data]
SC-28	Protection of Information at Rest	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	SC-28 [confidentiality and integrity] [confidential state data]
SC-28 (01)	Protection of Information at Rest | Cryptographic Protection	See FD for details. FD = NIST SP 800-53.	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(1) [system components that host confidential state data] [confidential state data]
SC-28 (01)	Protection of Information at Rest | Cryptographic Protection	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	SC-28(1) [system components that host confidential state data] [confidential state data]
SC-28 (01)	Protection of Information at Rest | Cryptographic Protection	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	SC-28(1) [system components that host confidential state data] [confidential state data]
SC-28 (01)	Protection of Information at Rest | Cryptographic Protection	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Encrypting Data In Storage Media	DCH-07.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	5	SC-28(1) [system components that host confidential state data] [confidential state data]
SC-39	Process Isolation	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Process Isolation	SEA-04	Mechanisms exist to implement a separate execution domain for each executing process.	10	
SI-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	SI-1 (c)(1) [least every three (3) years] and [following significant changes] SI-1 (c)(2) [at least annually] and [following significant changes]
SI-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	SI-1 (c)(1) [least every three (3) years] and [following significant changes] SI-1 (c)(2) [at least annually] and [following significant changes]
SI-01	Policy and Procedures	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	SI-1 (c)(1) [least every three (3) years] and [following significant changes] SI-1 (c)(2) [at least annually] and [following significant changes]
SI-02	Flaw Remediation	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	SI-2(c) [within 30 days of release of updates]
SI-02	Flaw Remediation	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	SI-2(c) [within 30 days of release of updates]
SI-02	Flaw Remediation	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5	SI-2(c) [within 30 days of release of updates]
SI-03	Malicious Code Protection	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	SI-3 (c) (1)-1 [at least weekly] SI-3 (c) (1)-2 [to include endpoints] SI-3 (c) (2) [to include alerting administrator or defined security personnel]
SI-03	Malicious Code Protection	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	SI-3 (c) (1)-1 [at least weekly] SI-3 (c) (1)-2 [to include endpoints] SI-3 (c) (2) [to include alerting administrator or defined security personnel]
SI-03	Malicious Code Protection	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	SI-3 (c) (1)-1 [at least weekly] SI-3 (c) (1)-2 [to include endpoints] SI-3 (c) (2) [to include alerting administrator or defined security personnel]
SI-03	Malicious Code Protection	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Heuristic / Nonsignature-Based Detection	END-04.4	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5	SI-3 (c) (1)-1 [at least weekly] SI-3 (c) (1)-2 [to include endpoints] SI-3 (c) (2) [to include alerting administrator or defined security personnel]
SI-03	Malicious Code Protection	See FD for details. FD = NIST SP 800-53.	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-3 (c) (1)-1 [at least weekly] SI-3 (c) (1)-2 [to include endpoints] SI-3 (c) (2) [to include alerting administrator or defined security personnel]
SI-03	Malicious Code Protection	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5	SI-3 (c) (1)-1 [at least weekly] SI-3 (c) (1)-2 [to include endpoints] SI-3 (c) (2) [to include alerting administrator or defined security personnel]
SI-03	Malicious Code Protection	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	SI-3 (c) (1)-1 [at least weekly] SI-3 (c) (1)-2 [to include endpoints] SI-3 (c) (2) [to include alerting administrator or defined security personnel]
SI-04	System Monitoring	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
SI-04	System Monitoring	See FD for details. FD = NIST SP 800-53.	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	
SI-04	System Monitoring	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	
SI-04	System Monitoring	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
SI-04 (04)	System Monitoring | Inbound and Outbound Communications Traffic	See FD for details. FD = NIST SP 800-53.	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-05	Security Alerts, Advisories, and Directives	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
SI-05	Security Alerts, Advisories, and Directives	See FD for details. FD = NIST SP 800-53.	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-05	Security Alerts, Advisories, and Directives	See FD for details. FD = NIST SP 800-53.	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	See FD for details. FD = NIST SP 800-53.	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	See FD for details. FD = NIST SP 800-53.	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	See FD for details. FD = NIST SP 800-53.	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	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Integrity Checks	END-06.1	Mechanisms exist to validate configurations through integrity checking of software and firmware.	10	SI-7(1) [to include security-relevant events]
SI-07 (07)	Software, Firmware, and Information Integrity | Integration of Detection and Response	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Endpoint Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.	10	
SI-10	Information Input Validation	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	SI-10 [application inputs that connect to datastores containing confidential state data]
SI-10	Information Input Validation	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	SI-10 [application inputs that connect to datastores containing confidential state data]
SI-11	Error Handling	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Error Handling	TDA-19	Mechanisms exist to handle error conditions by:(1) Identifying potentially security-relevant error conditions;(2) Generating error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited; and(3) Revealing error messages only to authorized personnel.	10	
SI-12	Information Management and Retention	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
SI-12	Information Management and Retention	See FD for details. FD = NIST SP 800-53.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to:(1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law;(2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and(3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	
SI-16	Memory Protection	See FD for details. FD = NIST SP 800-53.	Functional	Equal	Memory Protection	SEA-10	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	10	