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

Focal Document: NIST SP 800-82 R3 Guide to Operational Technology (OT) Security - HI
Focal Document U https://csrc.nist.gov/pubs/sp/800/82/r3/final
Published STRM U https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-82

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationsh ip	Notes
AC-01	Policy and Procedures	executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the access control policy and the associated access controls;b. Designate an [Assignment: organization-defined official] to	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient	5	
AC-01	Policy and Procedures	executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the access control policy and the associated access controls;b. Designate an [Assignment: organization-defined official] to	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	5	
AC-01	Policy and Procedures	executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the access control policy and the associated access controls;b. Designate an [Assignment: organization-defined official] to	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
AC-02	Account Management	use of accounts;h. Notify account managers and [Assignment: organization-defined personnel or roles] within:1. [Assignment: organization-defined time period] when accounts are no longer required;2. [Assignment: organization-defined time period] when	Functional	Intersects With	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	5	
AC-02	Account Management	use of accounts;h. Notify account managers and [Assignment: organization-defined personnel or roles] within:1. [Assignment: organization-defined time period] when accounts are no longer required;2. [Assignment: organization-defined time period] when	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-02	Account Management	use of accounts;h. Notify account managers and [Assignment: organization-defined personnel or roles] within:1. [Assignment: organization-defined time period] when accounts are no longer required;2. [Assignment: organization-defined time period] when	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
AC-02	Account Management	use of accounts;h. Notify account managers and [Assignment: organization-defined personnel or roles] within:1. [Assignment: organization-defined time period] when accounts are no longer required;2. [Assignment: organization-defined time period] when	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public	5	
AC-02(01)	Account Management | Automated System Account Management	Support the management of system accounts using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Automated System Account Management (Directory Services)	IAC-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5	
AC-02(02)	Account Management | Automated Temporary and Emergency Account	Automatically [Selection (one): remove; disable] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].	Functional	Equal	Removal of Temporary / Emergency Accounts	IAC-15.2	Automated mechanisms exist to disable or remove temporary and emergency accounts after an organization-defined time period for each type of account.	10	
AC-02(03)	Account Management | Disable Accounts	defined time period] when the accounts:a. Have expired;b. Are no longer associated with a user or individual;c. Are in violation of organizational policy; ord. Have been inactive for [Assignment: organization-	Functional	Equal	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	10	
AC-02(04)	Account Management | Automated Audit Actions	Automatically audit account creation, modification, enabling, disabling, and removal actions.	Functional	Equal	Automated Audit Actions	IAC-15.4	audit account creation, modification, enabling, disabling and removal actions and notify organization-defined personnel	10	
AC-02(05)	Account Management | Inactivity Logout	Require that users log out when [Assignment: organization-defined time period of expected inactivity or description of when to log out].	Functional	Equal	Session Lock	IAC-24	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	10	
AC-02(11)	Account Management | Usage Conditions	Enforce [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined system accounts].	Functional	Equal	Usage Conditions	IAC-15.8	Automated mechanisms exist to enforce usage conditions for users and/or roles.	10	
AC-02(12)	Account Management | Account Monitoring for Atypical Usage	a. Monitor system accounts for [Assignment: organization-defined atypical usage]; andb. Report atypical usage of system accounts to [Assignment: organization-defined personnel or roles].	Functional	Equal	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to	10	
AC-02(13)	Account Management | Disable Accounts for High-risk Individuals	Disable accounts of individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks].	Functional	Intersects With	High-Risk Terminations	HRS-09.2	Mechanisms exist to expedite the process of removing "high risk" individual's access to Technology Assets, Applications, Services	5	
AC-02(13)	Account Management | Disable Accounts for High-risk Individuals	Disable accounts of individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks].	Functional	Intersects With	Account Disabling for High Risk Individuals	IAC-15.6	Mechanisms exist to disable accounts immediately upon notification for users posing a significant risk to the organization.	5	
AC-03	Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
AC-03	Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public	5	
AC-03	Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
AC-03(11)	Access Enforcement | Restrict Access to Specific Information Types	Restrict access to data repositories containing [Assignment: organization-defined information types].	Functional	Equal	Sensitive / Regulated Data Access Enforcement	CFG-08	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to restrict access to sensitive/regulated	10	
AC-04	Information Flow Enforcement	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].	Functional	Equal	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only	10	
AC-04(04)	Information Flow Enforcement | Flow Control of Encrypted Information	control mechanisms] by [Selection (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information;	Functional	Equal	Content Check for Encrypted Data	NET-04.3	Mechanisms exist to prevent encrypted data from bypassing content-checking mechanisms.	10	
AC-05	Separation of Duties	a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; andb. Define system access authorizations to support separation of duties.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
AC-05	Separation of Duties	a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; andb. Define system access authorizations to support separation of duties.	Functional	Intersects With	Dual Authorization for Change	CHG-04.3	Mechanisms exist to enforce a two-person rule for implementing changes to critical Technology Assets, Applications and/or	5	
AC-05	Separation of Duties	a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; andb. Define system access authorizations to support separation of duties.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public	5	
AC-05	Separation of Duties	a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; andb. Define system access authorizations to support separation of duties.	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	
AC-06	Least Privilege	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the principle of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational	5	
AC-06	Least Privilege	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	

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-06(01)	Least Privilege | Authorize Access to Security Functions	Authorize access for [Assignment: organization-defined individuals or roles] to:a. [Assignment: organization-defined security functions (deployed in hardware, software, and firmware)]; andb. [Assignment: organization-defined security-relevant information].	Functional	Equal	Authorize Access to Security Functions	IAC-21.1	Mechanisms exist to limit access to security functions to explicitly-authorized privileged users.	10	
AC-06(02)	Least Privilege | Non-privileged Access for Nonsecurity Functions	Require that users of system accounts (or roles) with access to [Assignment: organization-defined security functions or security-relevant information] use non-privileged accounts or roles, when accessing nonsecurity functions.	Functional	Equal	Non-Privileged Access for Non-Security Functions	IAC-21.2	Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.	10	
AC-06(05)	Least Privilege | Privileged Accounts	Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].	Functional	Equal	Management Approval For Privileged Accounts	IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles.	10	
AC-06(07)	Least Privilege | Review of User Privileges	frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; andb. Reassign or remove privileges, if necessary, to correctly reflect	Functional	Equal	Periodic Review of Account Privileges	IAC-17	review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges	10	
AC-06(09)	Least Privilege | Log Use of Privileged Functions	Log the execution of privileged functions.	Functional	Equal	Auditing Use of Privileged Functions	IAC-21.4	Mechanisms exist to audit the execution of privileged functions.	10	
AC-06(10)	Least Privilege | Prohibit Non-privileged Users from Executing Privileged Functions	Prevent non-privileged users from executing privileged functions.	Functional	Equal	Prohibit Non-Privileged Users from Executing Privileged Functions	IAC-21.5	non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security	10	
AC-07	Unsuccessful Logon Attempts	lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined	Functional	Equal	Account Lockout	IAC-22	attempts by a user during an organization-defined time period and automatically locks the account when the maximum	10	
AC-08	System Use Notification	subject to criminal and civil penalties; and4. Use of the system indicates consent to monitoring and recording;b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or	Functional	Equal	System Use Notification (Logon Banner)	SEA-18	banners that display an approved system use notification message or banner before granting access to Technology Assets,	10	
AC-10	Concurrent Session Control	Limit the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].	Functional	Equal	Concurrent Session Control	IAC-23	Mechanisms exist to limit the number of concurrent sessions for each system account.	10	
AC-11	Device Lock	[Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended]; andb. Retain the device lock until the user reestablishes access	Functional	Intersects With	Session Lock	IAC-24	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	5	
AC-11(01)	Device Lock | Pattern-hiding Displays	Conceal, via the device lock, information previously visible on the display with a publicly viewable image.	Functional	Equal	Pattern-Hiding Displays	IAC-24.1	Mechanisms exist to implement pattern-hiding displays to conceal information previously visible on the display during the session lock.	10	
AC-12	Session Termination	Automatically terminate a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].	Functional	Equal	Session Termination	IAC-25	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	10	
AC-14	Permitted Actions Without Identification or Authentication	actions] that can be performed on the system without identification or authentication consistent with organizational mission and business functions; andb. Document and provide supporting rationale in the security plan for the system, user actions not requiring	Functional	Equal	Permitted Actions Without Identification or Authorization	IAC-26	document the supporting rationale for specific user actions that can be performed on a system without identification or	10	
AC-17	Remote Access	configuration/connection requirements, and implementation guidance for each type of remote access allowed; andb. Authorize each type of remote access to the system prior to allowing such	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	Employ automated mechanisms to monitor and control remote access methods.	Functional	Equal	Automated Monitoring & Control	NET-14.1	Automated mechanisms exist to monitor and control remote access sessions.	10	
AC-17(02)	Remote Access | Protection of Confidentiality and Integrity Using Encryption	Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	Functional	Equal	Protection of Confidentiality / Integrity Using Encryption	NET-14.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).	10	
AC-17(03)	Remote Access | Managed Access Control Points	Route remote accesses through authorized and managed network access control points.	Functional	Equal	Managed Access Control Points	NET-14.3	Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).	10	
AC-17(04)	Remote Access | Privileged Commands and Access	access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: [Assignment: organization-defined needs]; andb. Document the rationale for remote access in the security plan for the	Functional	Equal	Remote Privileged Commands & Sensitive Data Access	NET-14.4	execution of privileged commands and access to security-relevant information via remote access only for	10	
AC-17(09)	Remote Access | Disconnect or Disable Access	Provide the capability to disconnect or disable remote access to the system within [Assignment: organization-defined time period].	Functional	Equal	Expeditious Disconnect / Disable Capability	NET-14.8	Mechanisms exist to provide the capability to expeditiously disconnect or disable a user's remote access session.	10	
AC-17(10)	Remote Access | Authenticate Remote Commands	Implement [Assignment: organization-defined mechanisms] to authenticate [Assignment: organization-defined remote commands].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
AC-18	Wireless Access	a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; andb. Authorize each type of wireless access to the system prior to allowing such connections.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
AC-18	Wireless Access	a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; andb. Authorize each type of wireless access to the system prior to allowing such connections.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication	5	
AC-18(01)	Wireless Access | Authentication and Encryption	Protect wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.	Functional	Equal	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying	10	
AC-18(03)	Wireless Access | Disable Wireless Networking	Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.	Functional	Equal	Disable Wireless Networking	NET-15.2	unnecessary wireless networking capabilities that are internally embedded within system components prior to issuance to	10	
AC-18(04)	Wireless Access | Restrict Configurations by Users	Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.	Functional	Equal	Restrict Configuration By Users	NET-15.3	Mechanisms exist to identify and explicitly authorize users who are allowed to independently configure wireless networking capabilities.	10	
AC-18(05)	Wireless Access | Antennas and Transmission Power Levels	Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries.	Functional	Equal	Wireless Boundaries	NET-15.4	Mechanisms exist to confine wireless communications to organization-controlled boundaries.	10	
AC-19	Access Control for Mobile Devices	requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; andb. Authorize the connection of mobile devices to	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	10	
AC-19(05)	Access Control for Mobile Devices | Full Device or Container-based Encryption	Employ [Selection: full-device encryption; container-based encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].	Functional	Equal	Full Device & Container-Based Encryption	MDM-03	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.	10	
AC-20	Use of External Systems	the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:1. Access the system from external systems; and2.	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	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
AC-20(01)	Use of External Systems | Limits on Authorized Use	transmit organization-controlled information only after:a. Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; orb. Retention of approved	Functional	Equal	Limits of Authorized Use	DCH-13.1	Mechanisms exist to prohibit external parties, including Technology Assets, Applications and/or Services (TAAS), from	10	
AC-20(02)	Use of External Systems | Portable Storage Devices — Restricted Use	Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using [Assignment: organization-defined restrictions].	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
AC-21	Information Sharing	match the information's access and use restrictions for [Assignment: organization-defined information sharing circumstances where user discretion is required]; andb. Employ [Assignment: organization-defined automated mechanisms or manual processes] to assist	Functional	Intersects With	Information Sharing With Third Parties	PRI-07	Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data	5	
AC-22	Publicly Accessible Content	information does not contain nonpublic information;c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; andd. Review the content on the publicly accessible system	Functional	Equal	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	10	
AT-01	Policy and Procedures	regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;b. Designate an	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient	5	
AT-02	Literacy Training and Awareness	changes or following [Assignment: organization-defined events];b. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques];c. Update literacy training and awareness	Functional	Equal	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness	10	
AT-02(02)	Literacy Training and Awareness | Insider Threat	Provide literacy training on recognizing and reporting potential indicators of insider threat.	Functional	Equal	Insider Threat Awareness	THR-05	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.	10	
AT-02(03)	Literacy Training and Awareness | Social Engineering and Mining	Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.	Functional	Equal	Social Engineering & Mining	SAT-02.2	awareness training on recognizing and reporting potential and actual instances of social engineering and social	10	
AT-02(04)	and Awareness | Suspicious Communications and Anomalous	Provide literacy training on recognizing suspicious communications and anomalous behavior in organizational systems using [Assignment: organization-defined indicators of malicious code].	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-03.2	training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous	5	
AT-03	Role-based Training	system, information, or performing assigned duties, and [Assignment: organization-defined frequency] thereafter; and2. When required by system changes;b. Update role-based training content [Assignment:	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When security, compliance	5	
AT-04	Training Records	privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; andb. Retain individual training records for [Assignment: organization-defined	Functional	Equal	Security, Compliance & Resilience Training Records	SAT-04	and resilience awareness training; (2) Recurring awareness training; and	10	
AU-01	Policy and Procedures	standards, and guidelines; and2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;b. Designate an [Assignment:	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	5	
AU-01	Policy and Procedures	standards, and guidelines; and2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;b. Designate an [Assignment:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient	5	
AU-01	Policy and Procedures	standards, and guidelines; and2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;b. Designate an [Assignment:	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
AU-02	Event Logging	the selection criteria for events to be logged;c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-02a.) along with the frequency of (or situation requiring) logging	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	5	
AU-02	Event Logging	the selection criteria for events to be logged;c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-02a.) along with the frequency of (or situation requiring) logging	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related	5	
AU-03	Content of Audit Records	establishes the following:a. What type of event occurred;b. When the event occurred;c. Where the event occurred;d. Source of the event;e. Outcome of the event; andf. Identity of any individuals, subjects, or	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	10	
AU-03(01)	Content of Audit Records | Additional Audit Information	Generate audit records containing the following additional information: [Assignment: organization-defined additional information].	Functional	Intersects With	Sensitive Event Log Information	MON-03.1	Mechanisms exist to protect sensitive/regulated data contained in log files.	5	
AU-04	Audit Log Storage Capacity	Allocate audit log storage capacity to accommodate [Assignment: organization-defined audit log retention requirements].	Functional	Equal	Event Log Storage Capacity	MON-04	Mechanisms exist to allocate and proactively manage sufficient event log storage capacity to reduce the likelihood of such capacity being exceeded	10	
AU-04(01)	Audit Log Storage Capacity | Transfer to Alternate Storage	Transfer audit logs [Assignment: organization-defined frequency] to a different system, system component, or media other than the system or system component conducting the logging.	Functional	Intersects With	Event Log Backup on Separate Physical Systems / Components	MON-08.1	event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or	5	
AU-05	Response to Audit Logging Process Failures	a. Alert [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] in the event of an audit logging process failure; andb. Take the following additional actions: [Assignment: organization-defined additional actions]	Functional	Equal	Response To Event Log Processing Failures	MON-05	Mechanisms exist to alert appropriate personnel in the event of a log processing failure and take actions to remedy the disruption.	10	
AU-05(01)	Response to Audit Logging Process Failures | Storage Capacity Warning	defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated audit log storage volume reaches [Assignment: organization-defined percentage] of	Functional	Equal	Event Log Storage Capacity Alerting	MON-05.2	alert appropriate personnel when the allocated volume reaches an organization-defined percentage of maximum event log storage	10	
AU-05(02)	Response to Audit Logging Process Failures | Real-time Alerts	defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit logging failure events	Functional	Intersects With	Real-Time Alerts of Event Logging Failure	MON-05.1	Mechanisms exist to provide 24x7x365 near real-time alerting capability when an event log processing failure occurs.	5	
AU-06	Audit Record Review, Analysis, and Reporting	inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity;b. Report findings to [Assignment: organization-defined personnel or roles]; andc. Adjust the level of audit record review, analysis, and reporting within the	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related	5	
AU-06	Audit Record Review, Analysis, and Reporting	inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity;b. Report findings to [Assignment: organization-defined personnel or roles]; andc. Adjust the level of audit record review, analysis, and reporting within the	Functional	Intersects With	Audit Level Adjustments	MON-02.6	level of audit review, analysis and reporting based on evolving threat information from law enforcement, industry associations or other credible	5	
AU-06(01)	Audit Record Review, Analysis, and Reporting | Automated Process Integration	Integrate audit record review, analysis, and reporting processes using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Sensitive Event Log Information	MON-03.1	Mechanisms exist to protect sensitive/regulated data contained in log files.	5	
AU-06(03)	Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories	Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to	5	
AU-06(05)	Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records	[Selection (one or more): vulnerability scanning information; performance data; system monitoring information; [Assignment: organization-defined data/information collected from other sources]] to further enhance the ability to identify inappropriate or	Functional	Equal	Integration of Scanning & Other Monitoring Information	MON-02.3	records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further	10	
AU-06(06)	Audit Record Review, Analysis, and Reporting | Correlation with Physical Monitoring	Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.	Functional	Equal	Correlation with Physical Monitoring	MON-02.4	records with information obtained from monitoring physical access to further enhance the ability to identify	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
AU-07	Audit Record Reduction and Report Generation	report generation capability that:a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; andb. Does not alter the original content or	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	
AU-07(01)	Audit Record Reduction and Report Generation | Automatic Processing	Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: [Assignment: organization-defined fields within audit records].	Functional	Intersects With	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	5	
AU-08	Time Stamps	for audit records; andb. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include	Functional	Intersects With	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	5	
AU-08	Time Stamps	for audit records; andb. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include	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	5	
AU-09	Protection of Audit Information	a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; andb. Alert [Assignment: organization-defined personnel or roles] upon detection of unauthorized access, modification, or deletion of audit information.	Functional	Equal	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	10	
AU-09(02)	Protection of Audit Information | Store on Separate Physical Systems or Components	Store audit records [Assignment: organization-defined frequency] in a repository that is part of a physically different system or system component than the system or component being audited.	Functional	Intersects With	Event Log Backup on Separate Physical Systems / Components	MON-08.1	event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or	5	
AU-09(03)	Protection of Audit Information | Cryptographic Protection	Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.	Functional	Equal	Cryptographic Protection of Event Log Information	MON-08.3	Cryptographic mechanisms exist to protect the integrity of event logs and audit tools.	10	
AU-09(04)	Protection of Audit Information | Access by Subset of Privileged Users	Authorize access to management of audit logging functionality to only [Assignment: organization-defined subset of privileged users or roles].	Functional	Equal	Access by Subset of Privileged Users	MON-08.2	Mechanisms exist to restrict access to the management of event logs to privileged users with a specific business need.	10	
AU-10	Non-repudiation	Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [Assignment: organization-defined actions to be covered by non-repudiation].	Functional	Equal	Non-Repudiation	MON-09	Mechanisms exist to utilize a non-repudiation capability to protect against an individual falsely denying having performed a particular action.	10	
AU-11	Audit Record Retention	Retain audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention	Functional	Equal	Event Log Retention	MON-10	with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and	10	
AU-12	Audit Record Generation	system components];b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; andc. Generate audit	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	
AU-12(01)	Audit Record Generation | System-wide and Time-correlated Audit Trail	defined system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of	Functional	Equal	System-Wide / Time-Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.	10	
AU-12(03)	Audit Record Generation | Changes by Authorized Individuals	organization-defined individuals or roles] to change the logging to be performed on [Assignment: organization-defined system components] based on [Assignment: organization-defined selectable event criteria] within	Functional	Equal	Changes by Authorized Individuals	MON-02.8	Mechanisms exist to provide privileged users or roles the capability to change the auditing to be performed on specified	10	
CA-01	Policy and Procedures	standards, and guidelines; and2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls:b. Designate an [Assignment: organization-	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
CA-01	Policy and Procedures	standards, and guidelines; and2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls:b. Designate an [Assignment: organization-	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	5	
CA-01	Policy and Procedures	standards, and guidelines; and2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls:b. Designate an [Assignment: organization-	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient	5	
CA-02	Control Assessments	is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;d. Assess the controls in the system and its environment of operation [Assignment:	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	5	
CA-02	Control Assessments	is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;d. Assess the controls in the system and its environment of operation [Assignment:	Functional	Intersects With	Technical Verification	IAO-06	Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and	5	
CA-02	Control Assessments	is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;d. Assess the controls in the system and its environment of operation [Assignment:	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	project development to determine the extent to which the controls are implemented correctly, operating as intended	5	
CA-02	Control Assessments	is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;d. Assess the controls in the system and its environment of operation [Assignment:	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications	5	
CA-02	Control Assessments	is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;d. Assess the controls in the system and its environment of operation [Assignment:	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the	5	
CA-02(01)	Control Assessments | Independent Assessors	Employ independent assessors or assessment teams to conduct control assessments.	Functional	Equal	Assessor Independence	IAO-02.1	assessors or assessment teams have the appropriate independence to conduct security, compliance and/or	10	
CA-02(02)	Control Assessments | Specialized Assessments	announced; unannounced), [Selection (one or more): in-depth monitoring; security instrumentation; automated security test cases; vulnerability scanning; malicious user testing; insider threat assessment; performance and load testing; data leakage or data	Functional	Intersects With	Specialized Assessments	IAO-02.2	(4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.);	5	
CA-03	Information Exchange	agreement; service level agreements; user agreements; nondisclosure agreements; [Assignment: organization-defined type of agreement]];b. Document, as part of each exchange agreement, the interface	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics;	5	
CA-03(06)	Information Exchange | Transfer Authorizations	Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.	Functional	Equal	Transfer Authorizations	DCH-14.2	Mechanisms exist to verify that individuals or Technology Assets, Applications and/or Services (TAAS) transferring data between	10	
CA-05	Plan of Action and Milestones	deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; andb. Update existing plan of action and milestones [Assignment:	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	(4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection;	5	
CA-06	Authorization	authorizing official for the system, before commencing operations:1. Accepts the use of common controls inherited by the system; and2. Authorizes the system to operate;d. Ensure that the authorizing official for	Functional	Equal	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go	10	
CA-07	Continuous Monitoring	organization-defined frequencies] for assessment of control effectiveness;c. Ongoing control assessments in accordance with the continuous monitoring strategy;d. Ongoing monitoring of system and organization-defined metrics in accordance with the	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	security, compliance and resilience controls oversight function that reports to the organization's executive	5	
CA-07(01)	Continuous Monitoring | Independent Assessment	Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.	Functional	Intersects With	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned	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
CA-07(04)	Continuous Monitoring | Risk Monitoring	Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:a. Effectiveness monitoring;b. Compliance monitoring; andc. Change monitoring.	Functional	Equal	Risk Monitoring	RSK-11	the continuous monitoring strategy that includes monitoring the effectiveness of security, compliance and resilience	10	
CA-08	Penetration Testing	Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components].	Functional	Equal	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	10	
CA-09	Internal System Connections	internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;c. Terminate internal system connections after [Assignment: organization-	Functional	Equal	Internal System Connections	NET-05.2	through authorizing internal connections of systems and documenting, for each internal connection, the interface characteristics, security	10	
CM-01	Policy and Procedures	regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;b. Designate an	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
CM-01	Policy and Procedures	regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;b. Designate an	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	5	
CM-01	Policy and Procedures	regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;b. Designate an	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient	5	
CM-02	Baseline Configuration	of the system; andb. Review and update the baseline configuration of the system:1. [Assignment: organization-defined frequency];2. When required due to [Assignment: organization-defined circumstances];	Functional	Intersects With	Reviews & Updates	CFG-02.1	update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component	5	
CM-02	Baseline Configuration	of the system; andb. Review and update the baseline configuration of the system:1. [Assignment: organization-defined frequency];2. When required due to [Assignment: organization-defined circumstances];	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications	5	
CM-02(02)	Baseline Configuration | Automation Support for Accuracy and Currency	Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or	10	
CM-02(03)	Baseline Configuration | Retention of Previous Configurations	Retain [Assignment: organization-defined number] of previous versions of baseline configurations of the system to support rollback.	Functional	Equal	Retention Of Previous Configurations	CFG-02.3	Mechanisms exist to retain previous versions of baseline configuration to support roll back.	10	
CM-02(07)	Baseline Configuration | Configure Systems and Components for High-Risk Areas	defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; andb. Apply the following controls to the systems or components when the individuals	Functional	Equal	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more	10	
CM-03	Configuration Change Control	configuration-controlled changes to the system;e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period];f. Monitor and review activities associated with	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	configuration-controlled changes to the system;e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period];f. Monitor and review activities associated with	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
CM-03(01)	Configuration Change Control | Automated Documentation, Notification, and Prohibition of Changes	configuration-controlled changes to the system;e. system and request change approval;c. Highlight proposed changes to the system that have not been approved or disapproved within [Assignment: organization-defined time period];d. Prohibit changes	Functional	Equal	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	10	
CM-03(02)	Configuration Change Control | Testing, Validation, and Documentation of Changes	Test, validate, and document changes to the system before finalizing the implementation of the changes.	Functional	Intersects With	Control Functionality Verification	CHG-06	functionality of security, compliance and resilience controls following implemented changes to ensure applicable	5	
CM-03(04)	Configuration Change Control | Security and Privacy Representatives	Require [Assignment: organization-defined security and privacy representatives] to be members of the [Assignment: organization-defined configuration change control element].	Functional	Equal	Compliance & Resilience Representative for Asset Lifecycle	CHG-02.3	Mechanisms exist to include a cybersecurity and/or data protection representative in the configuration change control	10	
CM-03(06)	Configuration Change Control | Cryptography Management	Ensure that cryptographic mechanisms used to provide the following controls are under configuration management: [Assignment: organization-defined controls].	Functional	Equal	Cryptographic Management	CHG-02.5	assets involved in providing cryptographic protections according to the organization's configuration management	10	
CM-04	Impact Analyses	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.	Functional	Equal	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	10	
CM-04(01)	Impact Analyses | Separate Test Environments	Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or	Functional	Equal	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized	10	
CM-04(02)	Impact Analyses | Verification of Controls	after system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.	Functional	Equal	Technical Verification	IAO-06	Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and	10	
CM-05	Access Restrictions for Change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.	Functional	Intersects With	Governing Access Restriction for Change	END-03.2	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to Technology	5	
CM-05	Access Restrictions for Change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
CM-05(01)	Access Restrictions for Change | Automated Access Enforcement and Audit Records	a. Enforce access restrictions using [Assignment: organization-defined automated mechanisms]; andb. Automatically generate audit records of the enforcement actions.	Functional	Equal	Automated Access Enforcement / Auditing	CHG-04.1	Mechanisms exist to perform after-the-fact reviews of configuration change logs to discover any unauthorized changes.	10	
CM-06	Configuration Settings	common secure configurations];b. Implement the configuration settings;c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications	5	
CM-06	Configuration Settings	common secure configurations];b. Implement the configuration settings;c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-	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-06(01)	Configuration Settings | Automated Management, Application, and	Manage, apply, and verify configuration settings for [Assignment: organization-defined system components] using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or	5	
CM-06(02)	Configuration Settings | Respond to Unauthorized Changes	Take the following actions in response to unauthorized changes to [Assignment: organization-defined configuration settings]: [Assignment: organization-defined actions].	Functional	Equal	Respond To Unauthorized Changes	CFG-02.8	Mechanisms exist to respond to unauthorized changes to configuration settings as security incidents.	10	
CM-07	Least Functionality	organization-defined mission essential capabilities]; andb. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, software,	Functional	Equal	Least Functionality	CFG-03	systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or	10	
CM-07(01)	Least Functionality | Periodic Review	defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; andb. Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be	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	

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
CM-07(02)	Least Functionality | Prevent Program Execution	[Selection (one or more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and programs authorized to execute on the system];b. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; andc. Review and update the list of authorized software programs [Assignment: organization-defined	Functional	Intersects With	Prevent Program Execution	SEA-06	Automated mechanisms exist to prevent the execution of unauthorized software programs.	5	
CM-07(05)	Least Functionality | Authorized Software — Allow-by-exception	Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; andc. Review and update the list of authorized software programs [Assignment: organization-defined	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-08	System Component Inventory	components assigned to any other system];4. Is at the level of granularity deemed necessary for tracking and reporting; and5. Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:	5	
CM-08	System Component Inventory	components assigned to any other system];4. Is at the level of granularity deemed necessary for tracking and reporting; and5. Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed	Functional	Intersects With	Component Duplication Avoidance	AST-02.3	source and repository to provide a trusted source and accountability for approved and implemented system components that prevents assets	5	
CM-08(01)	System Component Inventory | Updates During Installation and Removal	Update the inventory of system components as part of component installations, removals, and system updates.	Functional	Equal	Updates During Installations / Removals	AST-02.1	Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades.	10	
CM-08(02)	System Component Inventory | Automated Maintenance	Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Configuration Management Database (CMDB)	AST-02.9	and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-	10	
CM-08(03)	Inventory | Automated Unauthorized Component	using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; andb. Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such	Functional	Intersects With	Automated Unauthorized Component Detection	AST-02.2	Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.	5	
CM-08(03)	Inventory | Automated Unauthorized Component	using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; andb. Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such	Functional	Intersects With	Software Installation Alerts	END-03.1	Mechanisms exist to generate an alert when new software is detected.	5	
CM-08(03)	Inventory | Automated Unauthorized Component	using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; andb. Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such	Functional	Intersects With	Unauthorized Installation Alerts	CFG-05.1	Mechanisms exist to configure systems to generate an alert when the unauthorized installation of software is detected.	5	
CM-08(04)	System Component Inventory | Accountability Information	Include in the system component inventory information, a means for identifying by [Selection (one or more): name; position; role], individuals responsible and accountable for administering those components.	Functional	Equal	Accountability Information	AST-03.1	capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory	10	
CM-09	Configuration Management Plan	identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;c. Defines the configuration items for the system and places the configuration items under configuration	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
CM-09	Configuration Management Plan	identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;c. Defines the configuration items for the system and places the configuration items under configuration	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	laws;b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; andc. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for	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	governing the installation of software by users;b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; andc. Monitor policy compliance	Functional	Intersects With	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5	
CM-12	Information Location	system components on which the information is processed and stored;b. Identify and document the users who have access to the system and system components where the information is processed and stored; andc. Document changes to the location (i.e.	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	
CM-12(01)	Information Location | Automated Tools to Support Information Location	use automated tools to identify [Assignment: organization-defined information by information type] on [Assignment: organization-defined system components] to ensure controls are in place to protect organizational information and individual privacy	Functional	Equal	Automated Tools to Support Information Location	DCH-24.1	type to ensure adequate security, compliance and resilience controls are in place to protect organizational	10	
CP-01	Policy and Procedures	regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;b. Designate an	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	5	
CP-01	Policy and Procedures	regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;b. Designate an	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,	10	
CP-01	Policy and Procedures	regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;b. Designate an	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient	5	
CP-02	Contingency Plan	contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];c. Coordinate contingency planning activities with incident handling	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,	10	
CP-02	Contingency Plan	contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];c. Coordinate contingency planning activities with incident handling	Functional	Intersects With	Ongoing Contingency Planning	BCD-06	Mechanisms exist to update contingency plans due to changes affecting: (1) People (e.g., personnel	5	
CP-02(01)	Contingency Plan | Coordinate with Related Plans	Coordinate contingency plan development with organizational elements responsible for related plans.	Functional	Equal	Coordinate with Related Plans	BCD-01.1	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	10	
CP-02(02)	Contingency Plan | Capacity Planning	Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.	Functional	Equal	Capacity Planning	CAP-03	capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist	10	
CP-02(03)	Contingency Plan | Resume Mission and Business Functions	Plan for the resumption of [Selection (one): all; essential] mission and business functions within [Assignment: organization-defined time period] of contingency plan activation.	Functional	Intersects With	Resume All Missions & Business Functions	BCD-02.1	Mechanisms exist to resume all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation.	5	
CP-02(03)	Contingency Plan | Resume Mission and Business Functions	Plan for the resumption of [Selection (one): all; essential] mission and business functions within [Assignment: organization-defined time period] of contingency plan activation.	Functional	Intersects With	Resume Essential Missions & Business Functions	BCD-02.3	Mechanisms exist to resume essential missions and business functions within an organization-defined time period of contingency plan activation.	5	
CP-02(05)	Contingency Plan | Continue Mission and Business Functions	Plan for the continuation of [Selection (one): all; essential] mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.	Functional	Equal	Continue Essential Mission & Business Functions	BCD-02.2	essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration at primary	10	
CP-02(08)	Contingency Plan | Identify Critical Assets	Identify critical system assets supporting [Selection (one): all; essential] mission and business functions.	Functional	Equal	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that	10	
CP-03	Contingency Training	Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility;2. When required by system changes; and3. [Assignment: organization-defined frequency] thereafter; andb. Review and update contingency training content	Functional	Equal	Contingency Training	BCD-03	Mechanisms exist to adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities.	10	
CP-03(01)	Contingency Training | Simulated Events	Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.	Functional	Equal	Simulated Events	BCD-03.1	Mechanisms exist to incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.	10	

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	[Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests].b. Review the contingency plan test results; andc. Initiate corrective	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5	
CP-04	Contingency Plan Testing	[Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests].b. Review the contingency plan test results; andc. Initiate corrective	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to	5	
CP-04(01)	Contingency Plan Testing | Coordinate with Related Plans	Coordinate contingency plan testing with organizational elements responsible for related plans.	Functional	Equal	Coordinated Testing with Related Plans	BCD-04.1	Mechanisms exist to coordinate contingency plan testing with internal and external elements responsible for related plans.	10	
CP-04(02)	Contingency Plan Testing | Alternate Processing Site	Test the contingency plan at the alternate processing site:a. To familiarize contingency personnel with the facility and available resources; andb. To evaluate the capabilities of the alternate processing site to support contingency operations.	Functional	Equal	Alternate Storage & Processing Sites	BCD-04.2	storage & processing sites to both familiarize contingency personnel with the facility and evaluate the capabilities of the	10	
CP-06	Alternate Storage Site	a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; andb. Ensure that the alternate storage site provides controls equivalent to that of the primary site.	Functional	Equal	Alternate Storage Site	BCD-08	alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of	10	
CP-06(01)	Alternate Storage Site | Separation from Primary Site	Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.	Functional	Equal	Separation from Primary Storage Site	BCD-08.1	Mechanisms exist to separate the alternate storage site from the primary storage site to reduce susceptibility to similar threats.	10	
CP-06(02)	Alternate Storage Site | Recovery Time and Recovery Point Objectives	Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
CP-06(03)	Alternate Storage Site | Accessibility	Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.	Functional	Equal	Primary Storage Site Accessibility	BCD-08.2	Mechanisms exist to identify and mitigate potential accessibility problems to the alternate storage sites in the event of an area-wide disruption or	10	
CP-07	Alternate Processing Site	time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable;b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put	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-07(01)	Alternate Processing Site | Separation from Primary Site	Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.	Functional	Equal	Separation from Primary Processing Site	BCD-09.1	Mechanisms exist to separate the alternate processing site from the primary processing site to reduce susceptibility to similar threats.	10	
CP-07(02)	Alternate Processing Site | Accessibility	Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	Functional	Equal	Alternate Processing Site Accessibility	BCD-09.2	Mechanisms exist to mitigate potential accessibility problems to the alternate processing sites and possible mitigation actions, in the event of an area-wide disruption or	10	
CP-07(03)	Alternate Processing Site | Priority of Service	Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).	Functional	Equal	Alternate Site Priority of Service	BCD-09.3	Mechanisms exist to address priority-of-service provisions in alternate processing and storage sites that support availability requirements, including Recovery Time Objectives	10	
CP-07(04)	Alternate Processing Site | Preparation for Use	Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions.	Functional	Equal	Preparation for Use	BCD-09.4	alternate processing alternate to support essential missions and business functions so that the alternate site is capable of being	10	
CP-08	Telecommunications Services	resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period] when the primary telecommunications	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-08(01)	Telecommunications Services | Priority of Service Provisions	provisions in accordance with availability requirements (including recovery time objectives); andb. Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or	Functional	Equal	Telecommunications Priority of Service Provisions	BCD-10.1	telecommunications service agreements contain priority-of-service provisions that support availability requirements,	10	
CP-08(02)	Telecommunications Services | Single Points of Failure	Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.	Functional	Intersects With	Telecommunications Services Availability	BCD-10	Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services.	5	
CP-08(03)	Telecommunications Services | Separation of Primary and Alternate Providers	Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.	Functional	Equal	Separation of Primary / Alternate Providers	BCD-10.2	alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility	10	
CP-08(04)	Telecommunications Services | Provider Contingency Plan	service providers to have contingency plans;b. Review provider contingency plans to ensure that the plans meet organizational contingency requirements; andc. Obtain evidence of contingency testing and training by providers [Assignment: organization-defined	Functional	Equal	Provider Contingency Plan	BCD-10.3	contractually-require external service providers to have contingency plans that meet organizational contingency	10	
CP-09	System Backup	information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];c. Conduct backups of system documentation, including	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	5	
CP-09(01)	System Backup | Testing for Reliability and Integrity	Test backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.	Functional	Equal	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	10	
CP-09(02)	System Backup | Test Restoration Using Sampling	Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.	Functional	Equal	Test Restoration Using Sampling	BCD-11.5	Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing.	10	
CP-09(03)	System Backup | Separate Storage for Critical Information	Store backup copies of [Assignment: organization-defined critical system software and other security-related information] in a separate facility or in a fire rated container that is not collocated with the operational system.	Functional	Equal	Separate Storage for Critical Information	BCD-11.2	backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system	10	
CP-09(05)	System Backup | Transfer to Alternate Storage Site	Transfer system backup information to the alternate storage site [Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives].	Functional	Equal	Transfer to Alternate Storage Site	BCD-11.6	storage site at a rate that is capable of meeting both Recovery Time Objectives (RTOs) and Recovery Point Objectives	10	
CP-09(08)	System Backup | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined backup information].	Functional	Equal	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	10	
CP-10	System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.	Functional	Intersects With	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or	5	
CP-10	System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets,	5	
CP-10	System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
CP-10(02)	System Recovery and Reconstitution | Transaction Recovery	Implement transaction recovery for systems that are transaction-based.	Functional	Equal	Transaction Recovery	BCD-12.1	Mechanisms exist to utilize specialized backup mechanisms that will allow transaction recovery for transaction-based	10	
CP-10(04)	System Recovery and Reconstitution | Restore Within Time Period	Provide the capability to restore system components within [Assignment: organization-defined restoration time periods] from configuration-controlled and integrity-protected information representing a known, operational state for the components.	Functional	Equal	Restore Within Time Period	BCD-12.4	Mechanisms exist to restore Technology Assets, Applications, Services and/or Data (TAASD) within organization-defined	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
CP-10(06)	System Recovery and Reconstitution | Component Protection	Protect system components used for recovery and reconstitution.	Functional	Equal	Backup & Restoration Hardware Protection	BCD-13	Mechanisms exist to protect backup and restoration hardware and software.	10	
CP-12	Safe Mode	When [Assignment: organization-defined conditions] are detected, enter a safe mode of operation with [Assignment: organization-defined restrictions of safe mode of operation].	Functional	Intersects With	Fail Secure	SEA-07.2	systems to fail to an organization-defined known-state for types of failures, preserving system state information in	5	
IA-01	Policy and Procedures	guidelines; and2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;b. Designate an [Assignment:	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	5	
IA-01	Policy and Procedures	guidelines; and2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;b. Designate an [Assignment:	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
IA-01	Policy and Procedures	guidelines; and2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;b. Designate an [Assignment:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient	5	
IA-02	Identification and Authentication (organizational Users)	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.	Functional	Equal	Identification & Authentication for Organizational Users	IAC-02	identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of	10	
IA-02(01)	Authentication (organizational Users) | Multi-factor Authentication to	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access;	5	
IA-02(01)	Authentication (organizational Users) | Multi-factor Authentication to	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Local Access to Privileged Accounts	IAC-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	5	
IA-02(01)	Authentication (organizational Users) | Multi-factor Authentication to	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Information Assurance Enabled Products	TDA-02.2	IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved	5	
IA-02(01)	Authentication (organizational Users) | Multi-factor Authentication to	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Out-of-Band Multi-Factor Authentication	IAC-06.4	for access to privileged and non-privileged accounts such that one of the factors is independently provided by a	5	
IA-02(01)	Authentication (organizational Users) | Multi-factor Authentication to	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5	
IA-02(01)	Authentication (organizational Users) | Multi-factor Authentication to	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Network Access to Non-Privileged Accounts	IAC-06.2	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts.	5	
IA-02(01)	Authentication (organizational Users) | Multi-factor Authentication to	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Hardware Token-Based Authentication	IAC-10.7	Automated mechanisms exist to ensure organization-defined token quality requirements are satisfied for hardware token-based authentication	5	
IA-02(02)	Authentication (organizational Users) | Multi-factor Authentication to Non-privileged	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Information Assurance Enabled Products	TDA-02.2	IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved	5	
IA-02(02)	Authentication (organizational Users) | Multi-factor Authentication to Non-privileged	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Network Access to Non-Privileged Accounts	IAC-06.2	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts.	5	
IA-02(02)	Authentication (organizational Users) | Multi-factor Authentication to Non-privileged	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Out-of-Band Multi-Factor Authentication	IAC-06.4	for access to privileged and non-privileged accounts such that one of the factors is independently provided by a	5	
IA-02(02)	Authentication (organizational Users) | Multi-factor Authentication to Non-privileged	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Hardware Token-Based Authentication	IAC-10.7	Automated mechanisms exist to ensure organization-defined token quality requirements are satisfied for hardware token-based authentication	5	
IA-02(02)	Authentication (organizational Users) | Multi-factor Authentication to Non-privileged	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5	
IA-02(02)	Authentication (organizational Users) | Multi-factor Authentication to Non-privileged	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access;	5	
IA-02(02)	Authentication (organizational Users) | Multi-factor Authentication to Non-privileged	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Local Access to Privileged Accounts	IAC-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	5	
IA-02(05)	Authentication (organizational Users) | Individual Authentication with Group	When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.	Functional	Equal	Group Authentication	IAC-02.1	Mechanisms exist to require individuals to be authenticated with an individual authenticator when a group authenticator is utilized	10	
IA-02(08)	Authentication (organizational Users) | Access to Accounts — Replay	Implement replay-resistant authentication mechanisms for access to [Selection (one or more): privileged accounts; non-privileged accounts].	Functional	Equal	Replay-Resistant Authentication	IAC-02.2	Automated mechanisms exist to employ replay-resistant authentication.	10	
IA-02(12)	Identification and Authentication (organizational Users) | Acceptance of PIV Credentials	Accept and electronically verify Personal Identity Verification-compliant credentials.	Functional	Intersects With	Acceptance of PIV Credentials	IAC-02.3	Mechanisms exist to accept and electronically verify organizational Personal Identity Verification (PIV) credentials.	5	
IA-03	Device Identification and Authentication	Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that	5	
IA-04	Identifier Management	personnel or roles] to assign an individual, group, role, service, or device identifier;b. Selecting an identifier that identifies an individual, group, role, service, or device;c. Assigning the identifier to the intended individual, group, role, service, or device; and	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External	5	
IA-04	Identifier Management	personnel or roles] to assign an individual, group, role, service, or device identifier;b. Selecting an identifier that identifies an individual, group, role, service, or device;c. Assigning the identifier to the intended individual, group, role, service, or device; and	Functional	Intersects With	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services	5	
IA-04(04)	Identifier Management | Identify User Status	Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External	5	
IA-04(04)	Identifier Management | Identify User Status	Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].	Functional	Intersects With	User Identity (ID) Management	IAC-09.1	Mechanisms exist to ensure proper user identification management for non-consumer users and administrators.	5	
IA-04(04)	Identifier Management | Identify User Status	Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].	Functional	Intersects With	Identity User Status	IAC-09.2	Mechanisms exist to identify contractors and other third-party users through unique username characteristics.	5	

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-05	Authenticator Management	procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;e. Changing default authenticators prior to first use;f. Changing or	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and	5	
IA-05	Authenticator Management	procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;e. Changing default authenticators prior to first use;f. Changing or refreshing authenticators [Assignment: organization-	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	passwords in IA-5(1)(a);c. Transmit passwords only over cryptographically-protected channels;d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;e. Require	Functional	Intersects With	Automated Support For Password Strength	IAC-10.4	Mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity	5	
IA-05(01)	Authenticator Management | Password-based Authentication	passwords in IA-5(1)(a);c. Transmit passwords only over cryptographically-protected channels;d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;e. Require	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication	5	
IA-05(01)	Authenticator Management | Password-based Authentication	passwords in IA-5(1)(a);c. Transmit passwords only over cryptographically-protected channels;d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;e. Require	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and	5	
IA-05(02)	Authenticator Management | Public Key-based Authentication	the individual or group; andb. When public key infrastructure (PKI) is used:1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate	Functional	Equal	PKI-Based Authentication	IAC-10.2	Mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for	10	
IA-05(06)	Authenticator Management | Protection of Authenticators	Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.	Functional	Intersects With	User Responsibilities for Account Management	IAC-18	Mechanisms exist to require users to follow accepted practices in the use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart	5	
IA-05(06)	Authenticator Management | Protection of Authenticators	Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access	5	
IA-06	Authentication Feedback	Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.	Functional	Equal	Authenticator Feedback	IAC-11	Mechanisms exist to obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized	10	
IA-07	Cryptographic Module Authentication	implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.	Functional	Intersects With	Cryptographic Module Authentication	IAC-12	Mechanisms exist to ensure cryptographic modules adhere to applicable statutory, regulatory and contractual requirements for security strength	5	
IA-07	Cryptographic Module Authentication	implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.	Functional	Intersects With	Automated Authentication Through Cryptographic Modules	CRY-02	Automated mechanisms exist to enable systems to authenticate to a cryptographic module.	5	
IA-08	Identification and Authentication (non-organizational Users)	Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.	Functional	Equal	Identification & Authentication for Non-Organizational Users	IAC-03	identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services	10	
IA-08(01)	Identification and Authentication (non-organizational Users) | Acceptance of PIV Credentials from Other	Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.	Functional	Equal	Acceptance of PIV Credentials from Other Organizations	IAC-03.1	Mechanisms exist to accept and electronically verify Personal Identity Verification (PIV) credentials from third-parties.	10	
IA-08(02)	Identification and Authentication (non-organizational Users) | Acceptance of External	a. Accept only external authenticators that are NIST-compliant; andb. Document and maintain a list of accepted external authenticators.	Functional	Equal	Acceptance of Third-Party Credentials	IAC-03.2	Automated mechanisms exist to accept Federal Identity, Credential and Access Management (FICAM)-approved third-party credentials	10	
IA-08(04)	Identification and Authentication (non-organizational Users) | Use of Defined Profiles	Conform to the following profiles for identity management [Assignment: organization-defined identity management profiles].	Functional	Equal	Use of FICAM-Issued Profiles	IAC-03.3	Mechanisms exist to conform systems to Federal Identity, Credential and Access Management (FICAM)-issued profiles	10	
IA-11	Re-authentication	Require users to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].	Functional	Equal	Re-Authentication	IAC-14	Mechanisms exist to force users and devices to re-authenticate according to organization-defined circumstances that necessitate re-authentication	10	
IA-12	Identity Proofing	access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;b. Resolve user identities to a unique individual; andc. Collect, validate, and verify	Functional	Equal	Identity Proofing (Identity Verification)	IAC-28	Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions.	10	
IA-12(01)	Identity Proofing | Supervisor Authorization	Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.	Functional	Intersects With	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts	5	
IA-12(02)	Identity Proofing | Identity Evidence	Require evidence of individual identification be presented to the registration authority.	Functional	Equal	Identity Evidence	IAC-28.2	Mechanisms exist to require evidence of individual identification to be presented to the registration authority.	10	
IA-12(03)	Identity Proofing | Identity Evidence Validation and Verification	Require that the presented identity evidence be validated and verified through [Assignment: organizational defined methods of validation and verification].	Functional	Equal	Identity Evidence Validation & Verification	IAC-28.3	Mechanisms exist to require that the presented identity evidence be validated and verified through organizational-defined methods of validation and verification	10	
IA-12(04)	Identity Proofing | In-person Validation and Verification	Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
IA-12(04)	Identity Proofing | In-person Validation and Verification	Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.	Functional	Intersects With	In-Person or Trusted Third-Party Registration	IAC-10.3	Mechanisms exist to conduct in-person or trusted third-party identify verification before user accounts for third-parties are created	5	
IA-12(04)	Identity Proofing | In-person Validation and Verification	Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.	Functional	Intersects With	In-Person Validation & Verification	IAC-28.4	Mechanisms exist to require that the validation and verification of identity evidence be conducted in person before a designated registration authority	5	
IA-12(05)	Identity Proofing | Address Confirmation	Require that a [Selection (one): registration code; notice of proofing] be delivered through an out-of-band channel to verify the users address (physical or digital) of record.	Functional	Equal	Address Confirmation	IAC-28.5	Mechanisms exist to require that a notice of proofing be delivered through an out-of-band channel to verify the user's address (physical or digital)	10	
IR-01	Policy and Procedures	executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;b. Designate an [Assignment: organization-defined	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient	5	
IR-01	Policy and Procedures	executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;b. Designate an [Assignment: organization-defined	Functional	Subset Of	Incident Response Operations	IRO-01	and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and	10	
IR-01	Policy and Procedures	executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;b. Designate an [Assignment: organization-defined	Functional	Intersects With	IRP Update	IRO-04.2	review and modify incident response practices to incorporate lessons learned, business process changes and industry	5	
IR-01	Policy and Procedures	executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;b. Designate an [Assignment: organization-defined	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of	5	
IR-01	Policy and Procedures	executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;b. Designate an [Assignment: organization-defined	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	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
IR-02	Incident Response Training	of assuming an incident response role or responsibility or acquiring system access;2. When required by system changes; and3. [Assignment: organization-defined frequency] thereafter; andb. Review and	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5	
IR-02(01)	Incident Response Training | Simulated Events	Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.	Functional	Equal	Simulated Incidents	IRO-05.1	Mechanisms exist to incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.	10	
IR-02(02)	Incident Response Training | Automated Training Environments	Provide an incident response training environment using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Automated Incident Response Training Environments	IRO-05.2	Automated mechanisms exist to provide a more thorough and realistic incident response training environment.	10	
IR-03	Incident Response Testing	Test the effectiveness of the incident response capability for the system [Assignment: organization-defined frequency] using the following tests: [Assignment: organization-defined tests].	Functional	Intersects With	Incident Response Testing	IRO-06	incident response capabilities through realistic exercises to determine the operational effectiveness of those	5	
IR-03(02)	Incident Response Testing | Coordination with Related Plans	Coordinate incident response testing with organizational elements responsible for related plans.	Functional	Equal	Coordination with Related Plans	IRO-06.1	Mechanisms exist to coordinate incident response testing with organizational elements responsible for related plans.	10	
IR-04	Incident Handling	incident handling activities with contingency planning activities;c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the	Functional	Equal	Incident Handling	IRO-02	(2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment;	10	
IR-04(01)	Incident Handling | Automated Incident Handling Processes	Support the incident handling process using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Automated Incident Handling Processes	IRO-02.1	Automated mechanisms exist to support the incident handling process.	10	
IR-04(04)	Incident Handling | Information Correlation	Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related	5	
IR-04(04)	Incident Handling | Information Correlation	Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to	5	
IR-04(11)	Incident Handling | Integrated Incident Response Team	Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in [Assignment: organization-defined time period].	Functional	Equal	Integrated Security Incident Response Team (ISIRT)	IRO-07	integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response	10	
IR-05	Incident Monitoring	Track and document incidents.	Functional	Equal	Situational Awareness For Incidents	IRO-09	monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through	10	
IR-05(01)	Incident Monitoring | Automated Tracking, Data Collection, and Analysis	Track incidents and collect and analyze incident information using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Automated Tracking, Data Collection & Analysis	IRO-09.1	assist in the tracking, collection and analysis of information from actual and potential cybersecurity and data	10	
IR-06	Incident Reporting	a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; andb. Report incident information to [Assignment: organization-defined authorities].	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and	5	
IR-06	Incident Reporting	a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; andb. Report incident information to [Assignment: organization-defined authorities].	Functional	Intersects With	Regulatory & Law Enforcement Contacts	IRO-14	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.	5	
IR-06	Incident Reporting	a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; andb. Report incident information to [Assignment: organization-defined authorities].	Functional	Intersects With	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	5	
IR-06(01)	Incident Reporting | Automated Reporting	Report incidents using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Automated Reporting	IRO-10.1	Automated mechanisms exist to assist in the reporting of cybersecurity and data protection incidents.	10	
IR-06(03)	Incident Reporting | Supply Chain Coordination	Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.	Functional	Intersects With	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity and data protection incident information to the provider of the Technology	5	
IR-07	Incident Response Assistance	Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.	Functional	Equal	Incident Reporting Assistance	IRO-11	Mechanisms exist to provide incident response advice and assistance to users of Technology Assets, Applications	10	
IR-07(01)	Assistance | Automation Support for Availability of Information and	Increase the availability of incident response information and support using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Automation Support of Availability of Information / Support	IRO-11.1	Automated mechanisms exist to increase the availability of incident response-related information and support.	10	
IR-08	Incident Response Plan	Addresses the sharing of incident information;9. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]; and10. Explicitly designates responsibility for incident response to [Assignment:	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	
MA-01	Policy and Procedures	Executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;b. Designate an [Assignment: organization-defined	Functional	Subset Of	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance	10	
MA-01	Policy and Procedures	Executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;b. Designate an [Assignment: organization-defined	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-01	Policy and Procedures	Executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;b. Designate an [Assignment: organization-defined	Functional	Intersects With	Auditing Remote Maintenance	MNT-05.1	remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote	5	
MA-01	Policy and Procedures	Executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;b. Designate an [Assignment: organization-defined	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	5	
MA-01	Policy and Procedures	Executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;b. Designate an [Assignment: organization-defined	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient	5	
MA-02	Controlled Maintenance	personnel or roles] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;d. Sanitize equipment to remove the following information from associated media prior to	Functional	Equal	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application	10	
MA-02(02)	Controlled Maintenance | Automated Maintenance Activities	repair, and replacement actions for the system using [Assignment: organization-defined automated mechanisms]; andb. Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process	Functional	Equal	Automated Maintenance Activities	MNT-02.1	Automated mechanisms exist to schedule, conduct and document maintenance and repairs.	10	
MA-03	Maintenance Tools	a. Approve, control, and monitor the use of system maintenance tools; andb. Review previously approved system maintenance tools [Assignment: organization-defined frequency].	Functional	Intersects With	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	5	
MA-03(01)	Maintenance Tools | Inspect Tools	Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.	Functional	Equal	Inspect Tools	MNT-04.1	Mechanisms exist to inspect maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.	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
MA-03(02)	Maintenance Tools | Inspect Media	Check media containing diagnostic and test programs for malicious code before the media are used in the system.	Functional	Equal	Inspect Media	MNT-04.2	Mechanisms exist to check media containing diagnostic and test programs for malicious code before the media are used.	10	
MA-03(03)	Maintenance Tools | Prevent Unauthorized Removal	that there is no organizational information contained on the equipment;b. Sanitizing or destroying the equipment;c. Retaining the equipment within the facility; ord. Obtaining an exemption from [Assignment: organization-defined personnel or roles]	Functional	Equal	Prevent Unauthorized Removal	MNT-04.3	Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational	10	
MA-04	Nonlocal Maintenance	with organizational policy and documented in the security plan for the system;c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;d. Maintain	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	with organizational policy and documented in the security plan for the system;c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;d. Maintain	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	with organizational policy and documented in the security plan for the system;c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;d. Maintain	Functional	Intersects With	Auditing Remote Maintenance	MNT-05.1	remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote	5	
MA-04(01)	Nonlocal Maintenance | Logging and Review	a. Log [Assignment: organization-defined audit events] for nonlocal maintenance and diagnostic sessions; andb. Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior.	Functional	Intersects With	Auditing Remote Maintenance	MNT-05.1	remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote	5	
MA-04(03)	Nonlocal Maintenance | Comparable Security and Sanitization	implemented on the system being serviced; ord. Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational information); and after the service is performed,	Functional	Equal	Remote Maintenance Comparable Security & Sanitization	MNT-05.6	Mechanisms exist to require Technology Assets, Applications and/or Services (TAAS) performing remote, non-local	10	
MA-05	Maintenance Personnel	maintenance organizations or personnel that do not have non-escorted personnel performing maintenance on the system possess the required access authorizations; andc. Designate organizational personnel with required access authorizations and technical competence to	Functional	Equal	Authorized Maintenance Personnel	MNT-06	Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.	10	
MA-05(01)	Maintenance Personnel | Individuals Without Appropriate Access	personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; and2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access	Functional	Intersects With	Maintenance Personnel Without Appropriate Access	MNT-06.1	risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are	5	
MA-06	Timely Maintenance	Obtain maintenance support and/or spare parts for [Assignment: organization-defined system components] within [Assignment: organization-defined time period] of failure.	Functional	Equal	Timely Maintenance	MNT-03	Mechanisms exist to obtain maintenance support and/or spare parts for Technology Assets, Applications and/or	10	
MA-07	Field Maintenance	Restrict or prohibit field maintenance on [Assignment: organization-defined systems or system components] to [Assignment: organization-defined trusted maintenance facilities].	Functional	Equal	Field Maintenance	MNT-08	Mechanisms exist to securely conduct field maintenance on geographically deployed assets.	10	
MP-01	Policy and Procedures	executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;b. Designate an [Assignment: organization-defined	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	5	
MP-01	Policy and Procedures	executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;b. Designate an [Assignment: organization-defined	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
MP-01	Policy and Procedures	Executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;b. Designate an [Assignment: organization-defined	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient	5	
MP-02	Media Access	Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	5	
MP-02	Media Access	Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	5	
MP-03	Media Marking	limitations, handling caveats, and applicable security markings (if any) of the information; andb. Exempt [Assignment: organization-defined types of system media] from marking if the media remain within	Functional	Intersects With	Media Marking	DCH-04	in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security	5	
MP-03	Media Marking	limitations, handling caveats, and applicable security markings (if any) of the information; andb. Exempt [Assignment: organization-defined types of system media] from marking if the media remain within	Functional	Intersects With	Automated Marking	DCH-04.1	files to indicate the distribution limitations, handling requirements and applicable security markings (if any) of the	5	
MP-04	Media Storage	organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; andb. Protect system media types defined in MP-4a until the media are destroyed or	Functional	Equal	Media Storage	DCH-06	digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are	10	
MP-05	Media Transport	custody of controlled areas using [Assignment: organization-defined controls];b. Maintain accountability for system media during transport outside of controlled areas;c. Document activities	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-06	Media Sanitization	media) prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; andb. Employ sanitization mechanisms with the strength and integrity commensurate with the	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	media) prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; andb. Employ sanitization mechanisms with the strength and integrity commensurate with the	Functional	Intersects With	System Media Sanitization	DCH-09	system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational	5	
MP-06	Media Sanitization	media) prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; andb. Employ sanitization mechanisms with the strength and integrity commensurate with the	Functional	Intersects With	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).	5	
MP-06(01)	Media Sanitization | Review, Approve, Track, Document, and Verify	Review, approve, track, document, and verify media sanitization and disposal actions.	Functional	Equal	System Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.	10	
MP-06(02)	Media Sanitization | Equipment Testing	Test sanitization equipment and procedures [Assignment: organization-defined frequency] to ensure that the intended sanitization is being achieved.	Functional	Equal	Equipment Testing	DCH-09.2	Mechanisms exist to test sanitization equipment and procedures to verify that the intended result is achieved.	10	
MP-06(03)	Media Sanitization | Nondestructive Techniques	portable storage devices prior to connecting such devices to the system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable	Functional	Intersects With	First Time Use Sanitization	DCH-09.4	Mechanisms exist to apply nondestructive sanitization techniques to portable storage devices prior to first use.	5	
MP-06(03)	Media Sanitization | Nondestructive Techniques	portable storage devices prior to connecting such devices to the system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable	Functional	Intersects With	System Media Sanitization	DCH-09	system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational	5	
MP-06(03)	Media Sanitization | Nondestructive Techniques	portable storage devices prior to connecting such devices to the system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable	Functional	Intersects With	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).	5	
MP-07	Media Use	[Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; andb. Prohibit the use of portable storage devices in organizational systems	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	

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-07	Media Use	[Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; andb. Prohibit the use of portable storage devices in organizational systems	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	[Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; andb. Prohibit the use of portable storage devices in organizational systems	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	5	
PE-01	Policy and Procedures	Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;b. Designate an [Assignment: organization-	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient	5	
PE-01	Policy and Procedures	Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;b. Designate an [Assignment: organization-	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
PE-01	Policy and Procedures	Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;b. Designate an [Assignment: organization-	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	5	
PE-02	Physical Access Authorizations	resides;b. Issue authorization credentials for facility access;c. Review the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; andd. Remove	Functional	Equal	Physical Access Authorizations	PES-02	current list of personnel with authorized access to organizational facilities (except for those areas within the facility	10	
PE-03	Physical Access Control	access to areas within the facility designated as publicly accessible by implementing the following controls: [Assignment: organization-defined physical access controls];d. Escort visitors and control visitor activity [Assignment: organization-defined	Functional	Intersects With	Physical Access Control	PES-03	physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility	5	
PE-03(01)	Physical Access Control | System Access	Enforce physical access authorizations to the system in addition to the physical access controls for the facility at [Assignment: organization-defined physical spaces containing one or more components of the system].	Functional	Equal	Access To Critical Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulated	10	
PE-04	Access Control for Transmission	Control physical access to [Assignment: organization-defined system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security controls].	Functional	Equal	Transmission Medium Security	PES-12.1	exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or	10	
PE-05	Access Control for Output Devices	Control physical access to output from [Assignment: organization-defined output devices] to prevent unauthorized individuals from obtaining the output.	Functional	Equal	Access Control for Output Devices	PES-12.2	exist to restrict access to printers and other system output devices to prevent unauthorized individuals from obtaining the	10	
PE-06	Monitoring Physical Access	security incidents;b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; andc.	Functional	Equal	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	10	
PE-06(01)	Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment	Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.	Functional	Equal	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	10	
PE-06(04)	Monitoring Physical Access | Monitoring Physical Access to Systems	Monitor physical access to the system in addition to the physical access monitoring of the facility at [Assignment: organization-defined physical spaces containing one or more components of the system].	Functional	Equal	Monitoring Physical Access To Critical Systems	PES-05.2	Facility security mechanisms exist to monitor physical access to critical systems or sensitive/regulated data, in	10	
PE-08	Visitor Access Records	the system resides for [Assignment: organization-defined time period];b. Review visitor access records [Assignment: organization-defined frequency]; andc. Report anomalies in visitor access records to	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-08(01)	Visitor Access Records | Automated Records Maintenance and Review	Maintain and review visitor access records using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Automated Records Management & Review	PES-06.4	Automated mechanisms exist to facilitate the maintenance and review of visitor access records.	10	
PE-09	Power Equipment and Cabling	Protect power equipment and power cabling for the system from damage and destruction.	Functional	Equal	Supporting Utilities	PES-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	10	
PE-10	Emergency Shutoff	system components] in emergency situations;b. Place emergency shutoff switches or devices in [Assignment: organization-defined location by system or system component] to facilitate access for authorized	Functional	Equal	Emergency Shutoff	PES-07.2	(1) Placing emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel; and	10	
PE-11	Emergency Power	Provide an uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the system; transition of the system to long-term alternate power] in the event of a primary power source loss.	Functional	Intersects With	Emergency Power	PES-07.3	exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary	5	
PE-11(01)	Emergency Power | Alternate Power Supply — Minimal Operational Capability	Provide an alternate power supply for the system that is activated [Selection (one): manually; automatically] and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.	Functional	Intersects With	Emergency Power	PES-07.3	exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary	5	
PE-12	Emergency Lighting	Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	Functional	Equal	Emergency Lighting	PES-07.4	automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and	10	
PE-13	Fire Protection	Employ and maintain fire detection and suppression systems that are supported by an independent energy source.	Functional	Equal	Fire Protection	PES-08	exist to utilize and maintain fire suppression and detection devices/systems for the system that are supported by an	10	
PE-13(01)	Fire Protection | Detection Systems — Automatic Activation and Notification	Employ fire detection systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders] in the event of a fire.	Functional	Equal	Fire Detection Devices	PES-08.1	exist to utilize and maintain fire detection devices/systems that activate automatically and notify organizational personnel and emergency responders in the	10	
PE-13(02)	Fire Suppression Systems — Automatic Activation and	automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders]; andb. Employ an automatic fire suppression capability when	Functional	Intersects With	Automatic Fire Suppression	PES-08.3	Facility security mechanisms exist to employ an automatic fire suppression capability for critical systems when the facility is not	5	
PE-14	Environmental Controls	humidity, pressure, radiation, [Assignment: organization-defined environmental control]] levels within the facility where the system resides at [Assignment: organization-defined acceptable levels]; andb. Monitor environmental control levels	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	Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.	Functional	Equal	Water Damage Protection	PES-07.5	exist to protect systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly and	10	
PE-15(01)	Water Damage Protection | Automation Support	Detect the presence of water near the system and alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Automation Support for Water Damage Protection	PES-07.6	Facility security mechanisms exist to detect the presence of water in the vicinity of critical systems and alert facility	10	
PE-16	Delivery and Removal	a. Authorize and control [Assignment: organization-defined types of system components] entering and exiting the facility; andb. Maintain records of the system components.	Functional	Equal	Delivery & Removal	PES-10	exist to isolate information processing facilities from points such as delivery and loading areas and other points to avoid	10	
PE-17	Alternate Work Site	use by employees;b. Employ the following controls at alternate work sites: [Assignment: organization-defined controls];c. Assess the effectiveness of controls at alternate work sites; andd. Provide a means for	Functional	Equal	Alternate Work Site	PES-11	Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.	10	
PE-18	Location of System Components	Position system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access.	Functional	Intersects With	Equipment Siting & Protection	PES-12	components within the facility to minimize potential damage from physical and environmental hazards and to minimize the	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
PE-22	Component Marking	Mark [Assignment: organization-defined system hardware components] indicating the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and	5	
PE-22	Component Marking	Mark [Assignment: organization-defined system hardware components] indicating the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.	Functional	Intersects With	Component Marking	PES-16	exist to mark system hardware components indicating the impact or classification level of the information permitted to be processed, stored or transmitted.	5	
PL-01	Policy and Procedures	[Assignment: organization-defined official] to manage executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;b. Designate an	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
PL-01	Policy and Procedures	[Assignment: organization-defined official] to manage executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;b. Designate an	Functional	Subset Of	Technology Development & Acquisition	TDA-01	implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet	10	
PL-01	Policy and Procedures	[Assignment: organization-defined official] to manage executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;b. Designate an	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	5	
PL-01	Policy and Procedures	[Assignment: organization-defined official] to manage executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;b. Designate an	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient	5	
PL-02	System Security and Privacy Plans	[Assignment: organization-defined official] to manage and privacy requirements for the system;11. Identify any relevant control baselines or overlays, if applicable;12. Describe the controls in place or planned for meeting the security and privacy	Functional	Intersects With	Plan / Coordinate with Other Organizational Entities	IAO-03.1	Assurance Program (IAP) activities with affected stakeholders before conducting such activities in order to reduce	5	
PL-02	System Security and Privacy Plans	and privacy requirements for the system;11. Identify any relevant control baselines or overlays, if applicable;12. Describe the controls in place or planned for meeting the security and privacy	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:	5	
PL-02	System Security and Privacy Plans	and privacy requirements for the system;11. Identify any relevant control baselines or overlays, if applicable;12. Describe the controls in place or planned for meeting the security and privacy	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	(1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network	5	
PL-04	Rules of Behavior	Establish and provide to individuals requiring access to the system, group, or application, the rules that describe their responsibilities and expected behavior with regard to information and system usage;2. Receive from individuals, prior to	Functional	Intersects With	Terms of Employment	HRS-05	employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant	5	
PL-04	Rules of Behavior	Establish and provide to individuals requiring access to the system, group, or application, the rules that describe their responsibilities and expected behavior with regard to information and system usage;2. Receive from individuals, prior to	Functional	Intersects With	Rules of Behavior	HRS-05.1	acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable	5	
PL-04	Rules of Behavior	Establish and provide to individuals requiring access to the system, group, or application, the rules that describe their responsibilities and expected behavior with regard to information and system usage;2. Receive from individuals, prior to	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies	5	
PL-04(01)	Rules of Behavior | Social Media and External Site/application Usage Restrictions	Establish and provide to individuals requiring access to the system, group, or application, the rules that describe their responsibilities and expected behavior with regard to information and system usage;2. Receive from individuals, prior to	Functional	Equal	Social Media & Social Networking Restrictions	HRS-05.2	of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on	10	
PL-08	Security and Privacy Architectures	Develop organization-wide architectures that:1. Describe how the architectures are integrated into and support the enterprise architecture; and2. Describe how the architectures are integrated into and support the enterprise	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	with industry-recognized leading practices, with consideration for security, compliance and resilience principles that	5	
PL-10	Baseline Selection	Select a control baseline for the system.	Functional	Equal	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications	10	
PL-11	Baseline Tailoring	Tailor the selected control baseline by applying specified tailoring actions.	Functional	Equal	Baseline Tailoring	CFG-02.9	actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or	10	
PM-01	Information Security Program Plan	Develop and disseminate an organization-wide information security program plan that:1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
PM-01	Information Security Program Plan	Develop and disseminate an organization-wide information security program plan that:1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or	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	5	
PM-01	Information Security Program Plan	Develop and disseminate an organization-wide information security program plan that:1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient	5	
PM-02	Information Security Program Leadership Role	Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide	5	
PM-03	Information Security and Privacy Resources	Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document exceptions to this requirement;b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable	Functional	Equal	Security, Compliance & Resilience Resource Management	PRM-02	requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and	10	
PM-04	Plan of Action and Milestones Process	Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation;2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and3. Are reported in accordance with	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
PM-04	Plan of Action and Milestones Process	Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and3. Are reported in accordance with	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	(4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection;	5	
PM-05	System Inventory	Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management	5	
PM-05	System Inventory	Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:	5	
PM-06	Measures of Performance	Develop, monitor, and report on the results of information security and privacy measures of performance.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide	5	
PM-06	Measures of Performance	Develop, monitor, and report on the results of information security and privacy measures of performance.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
PM-07	Enterprise Architecture	Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	with industry-recognized leading practices, with consideration for security, compliance and resilience principles that	5	
PM-08	Critical Infrastructure Plan	Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets,	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
PM-08	Critical Infrastructure Plan	Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
PM-09	Risk Management Strategy	systems; and2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information;b. Implement the risk management strategy consistently across the	Functional	Equal	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
PM-10	Authorization Process	those systems operate through authorization processes;b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; andc. Integrate the	Functional	Equal	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
PM-11	Mission and Business Process Definition	operations, organizational assets, individuals, other organizations, and the Nation; andb. Determine information protection and personally identifiable information processing needs arising from the defined	Functional	Equal	Business Process Definition	PRM-06	(1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs	10	
PM-12	Insider Threat Program	Implement an insider threat program that includes a cross-discipline insider threat incident handling team.	Functional	Equal	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross-discipline insider threat incident handling team.	10	
PM-13	Security and Privacy Workforce	Establish a security and privacy workforce development and improvement program.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
PM-13	Security and Privacy Workforce	Establish a security and privacy workforce development and improvement program.	Functional	Intersects With	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	
PM-14	Testing, Training, and Monitoring	privacy testing, training, and monitoring activities associated with organizational systems:1. Are developed and maintained; and2. Continue to be executed; andb. Review testing, training, and	Functional	Intersects With	Personal Data (PD) Control Testing, Training & Monitoring	PRI-08	Mechanisms exist to conduct testing, training and monitoring activities for Personal Data (PD) controls.	5	
PM-14	Testing, Training, and Monitoring	privacy testing, training, and monitoring activities associated with organizational systems:1. Are developed and maintained; and2. Continue to be executed; andb. Review testing, training, and	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	security, compliance and resilience controls oversight function that reports to the organization's executive	5	
PM-15	Security and Privacy Groups and Associations	privacy communities;a. To facilitate ongoing security and privacy education and training for organizational personnel;b. To maintain currency with recommended security and privacy practices, techniques, and	Functional	Intersects With	Threat Intelligence Program	THR-01	information-sharing capability that can influence the development of the system and security architectures, selection	5	
PM-15	Security and Privacy Groups and Associations	privacy communities;a. To facilitate ongoing security and privacy education and training for organizational personnel;b. To maintain currency with recommended security and privacy practices, techniques, and technologies; andc. To share current security and	Functional	Intersects With	Contacts With Groups & Associations	GOV-07	protection education and training for organizational personnel; (2) Maintain currency with recommended cybersecurity and	5	
PM-16	Threat Awareness Program	Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.	Functional	Intersects With	Threat Intelligence Program	THR-01	information-sharing capability that can influence the development of the system and security architectures, selection	5	
PM-17	Protecting Controlled Unclassified Information on External Systems	unclassified information that is processed, stored or transmitted on external systems, are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards; andb.	Functional	Equal	/ Regulated Data on External Technology Assets, Applications and/or	DCH-13.3	Mechanisms exist to ensure that the requirements for the protection of sensitive/regulated data processed, stored or	10	
PM-18	Privacy Program Plan	of other privacy officials and staff and their responsibilities;4. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program;5. Reflects coordination among organizational entities responsible	Functional	Equal	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to	10	
PM-19	Privacy Program Leadership Role	Appoint a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program	Functional	Equal	Chief Privacy Officer (CPO)	PRI-01.1	mission, accountability and resources to coordinate, develop and implement, applicable data privacy requirements and	10	
PM-20	Dissemination of Privacy Program Information	has access to information about organizational privacy activities and can communicate with its senior agency official for privacy;b. Ensures that organizational privacy practices and reports are publicly available;	Functional	Equal	Dissemination of Data Privacy Program Information	PRI-01.3	publicly available through organizational websites or document repositories; (3) Utilize publicly facing email addresses and/or phone lines to	10	
PM-20(01)	Privacy Program Information | Privacy Policies on Websites, Applications, and	organized in a way that is easy to understand and navigate;b. Provide information needed by the public to make an informed decision about whether and how to interact with the organization; andc. Are updated whenever the organization makes a substantive	Functional	Equal	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization	10	
PM-21	Accounting of Disclosures	information of the individual or organization to which the disclosure was made;b. Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years	Functional	Equal	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:	10	
PM-22	Personally Identifiable Information Quality Management	identifiable information across the information life cycle;b. Correcting or deleting inaccurate or outdated personally identifiable information;c. Disseminating notice of corrected or deleted personally identifiable	Functional	Intersects With	Data Quality Management	PRI-10	quality, utility, objectivity, integrity and impact determination and de-identification of	5	
PM-22	Personally Identifiable Information Quality Management	identifiable information across the information life cycle;b. Correcting or deleting inaccurate or outdated personally identifiable information;c. Disseminating notice of corrected or deleted personally identifiable	Functional	Intersects With	Data Quality Operations	DCH-22	Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of	5	
PM-23	Data Governance Body	Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].	Functional	Intersects With	Data Management Board	PRI-13	Mechanisms exist to establish a written charter for a Data Management Board (DMB) and assigned organization-defined	5	
PM-23	Data Governance Body	Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].	Functional	Intersects With	Data Quality Management	PRI-10	quality, utility, objectivity, integrity and impact determination and de-identification of	5	
PM-23	Data Governance Body	Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].	Functional	Intersects With	Data Governance	GOV-10	organization's policies, standards and procedures so that sensitive/regulated data is effectively managed and	5	
PM-24	Data Integrity Board	Establish a Data Integrity Board to:a. Review proposals to conduct or participate in a matching program; andb. Conduct an annual review of all matching programs in which the agency has participated.	Functional	Intersects With	Data Governance	GOV-10	organization's policies, standards and procedures so that sensitive/regulated data is effectively managed and	5	
PM-24	Data Integrity Board	Establish a Data Integrity Board to:a. Review proposals to conduct or participate in a matching program; andb. Conduct an annual review of all matching programs in which the agency has participated.	Functional	Intersects With	Data Management Board	PRI-13	Mechanisms exist to establish a written charter for a Data Management Board (DMB) and assigned organization-defined	5	
PM-24	Data Integrity Board	Establish a Data Integrity Board to:a. Review proposals to conduct or participate in a matching program; andb. Conduct an annual review of all matching programs in which the agency has participated.	Functional	Intersects With	Data Quality Management	PRI-10	quality, utility, objectivity, integrity and impact determination and de-identification of	5	
PM-24	Data Integrity Board	Establish a Data Integrity Board to:a. Review proposals to conduct or participate in a matching program; andb. Conduct an annual review of all matching programs in which the agency has participated.	Functional	Intersects With	Personal Data (PD) Accuracy & Integrity	PRI-05.2	Mechanisms exist to ensure the accuracy and relevance of Personal Data (PD) throughout the information lifecycle by:	5	
PM-24	Data Integrity Board	Establish a Data Integrity Board to:a. Review proposals to conduct or participate in a matching program; andb. Conduct an annual review of all matching programs in which the agency has participated.	Functional	Intersects With	Computer Matching Agreements (CMA)	PRI-02.3	Mechanisms exist to publish Computer Matching Agreements (CMA) on the organization's public website(s).	5	
PM-24	Data Integrity Board	Establish a Data Integrity Board to:a. Review proposals to conduct or participate in a matching program; andb. Conduct an annual review of all matching programs in which the agency has participated.	Functional	Intersects With	Automated Data Management Processes	PRI-02.2	Automated mechanisms exist to adjust data that is able to be collected, received, processed, stored, transmitted, shared,	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
PM-25	Personally Identifiable Information Used in Testing, Training,	and research;b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;c. Authorize the use of personally identifiable information when such information is required for internal testing,	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data	5	
PM-25	Personally Identifiable Information Used in Testing, Training,	and research;b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;c. Authorize the use of personally identifiable information when such information is required for internal testing,	Functional	Intersects With	Collection Minimization	END-13.3	Mechanisms exist to utilize sensors that are configured to minimize the collection of information about individuals.	5	
PM-25	Personally Identifiable Information Used in Testing, Training,	and research;b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;c. Authorize the use of personally identifiable information when such information is required for internal testing,	Functional	Intersects With	Minimize Visitor Personal Data (PD)	PES-06.5	Mechanisms exist to minimize the collection of Personal Data (PD) contained in visitor access records.	5	
PM-25	Personally Identifiable Information Used in Testing, Training,	and research;b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;c. Authorize the use of personally identifiable information when such information is required for internal testing,	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that:	5	
PM-25	Personally Identifiable Information Used in Testing, Training,	and research;b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;c. Authorize the use of personally identifiable information when such information is required for internal testing,	Functional	Intersects With	Limit Sensitive / Regulated Data In Testing, Training & Research	DCH-18.2	the use of sensitive/regulated data for research, testing, or training, in accordance with authorized, legitimate business	5	
PM-26	Complaint Management	necessary for successfully filing complaints;c. Tracking mechanisms to ensure all complaints received are reviewed and addressed within [Assignment: organization-defined time period];d. Acknowledgement	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or	5	
PM-26	Complaint Management	necessary for successfully filing complaints;c. Tracking mechanisms to ensure all complaints received are reviewed and addressed within [Assignment: organization-defined time period];d. Acknowledgement	Functional	Intersects With	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.	5	
PM-27	Privacy Reporting	organization-defined oversight bodies] to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and2. [Assignment: organization-defined officials] and other personnel with responsibility for monitoring privacy program	Functional	Equal	Documenting Data Processing Activities	PRI-14	Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage,	10	
PM-28	Risk Framing	and risk monitoring;3. Priorities and trade-offs considered by the organization for managing risk; and4. Organizational risk tolerance;b. Distribute the results of risk framing activities to [Assignment:	Functional	Equal	Risk Framing	RSK-01.1	(2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk	10	
PM-29	Risk Management Program Leadership Roles	security and privacy management processes with strategic, operational, and budgetary planning processes; andb. Establish a Risk Executive (function) to view and analyze risk from an organization-wide	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development,	5	
PM-29	Risk Management Program Leadership Roles	security and privacy management processes with strategic, operational, and budgetary planning processes; andb. Establish a Risk Executive (function) to view and analyze risk from an organization-wide	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide	5	
PM-29	Risk Management Program Leadership Roles	security and privacy management processes with strategic, operational, and budgetary planning processes; andb. Establish a Risk Executive (function) to view and analyze risk from an organization-wide	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
PM-30	Supply Chain Risk Management Strategy	acquisition, maintenance, and disposal of systems, system components, and system services;b. Implement the supply chain risk management strategy consistently across the organization; andc. Review and update the supply chain risk management strategy on	Functional	Equal	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development,	10	
PM-30(01)	Management Strategy | Suppliers of Critical or Mission-essential	Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.	Functional	Intersects With	Customized Development of Critical Components	TDA-12	Mechanisms exist to custom-develop critical system components, when Commercial Off The Shelf (COTS) solutions are unavailable	5	
PM-30(01)	Management Strategy | Suppliers of Critical or Mission-essential	Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.	Functional	Intersects With	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality	5	
PM-30(01)	Management Strategy | Suppliers of Critical or Mission-essential	Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications	5	
PM-31	Continuous Monitoring Strategy	organization-defined assessment frequencies] for control effectiveness; c. Ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy;d. Correlation and	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
PM-32	Purposing	Analyze [Assignment: organization-defined systems or systems components] supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose	Functional	Equal	Purpose Validation	GOV-11	Mechanisms exist to monitor mission/business-critical Technology Assets, Applications and/or Services (TAAS) to ensure	10	
PS-01	Policy and Procedures	regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;b. Designate an [Assignment:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient	5	
PS-01	Policy and Procedures	regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;b. Designate an [Assignment:	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	5	
PS-01	Policy and Procedures	regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;b. Designate an [Assignment:	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
PS-02	Position Risk Designation	a. Assign a risk designation to all organizational positions;b. Establish screening criteria for individuals filling those positions; andc. Review and update position risk designations [Assignment: organization-defined frequency]	Functional	Intersects With	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
PS-02	Position Risk Designation	a. Assign a risk designation to all organizational positions;b. Establish screening criteria for individuals filling those positions; andc. Review and update position risk designations [Assignment: organization-defined frequency]	Functional	Intersects With	Position Categorization	HRS-02	personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals	5	
PS-03	Personnel Screening	a. Screen individuals prior to authorizing access to the system; andb. Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening]	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	authenticators and credentials associated with the individual;c. Conduct exit interviews that include a discussion of [Assignment: organization-defined information security topics];d. Retrieve all security-related	Functional	Equal	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	10	
PS-04(02)	Personnel Termination | Automated Actions	use [Assignment: organization-defined automated mechanisms] to [Selection (one or more): notify [Assignment: organization-defined personnel or roles] of individual termination actions; disable access to system resources]	Functional	Equal	Automated Employment Status Notifications	HRS-09.4	notify Identity and Access Management (IAM) personnel or roles upon termination of an individual employment or	10	
PS-05	Personnel Transfer	organization;b. Initiate [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action];c. Modify access authorization as needed to correspond with any	Functional	Equal	Personnel Transfer	HRS-08	Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or	10	
PS-06	Access Agreements	frequency]; andc. Verify that individuals requiring access to organizational information and systems:1. Sign appropriate access agreements prior to being granted access; and2. Re-sign access agreements to	Functional	Intersects With	Confidentiality Agreements	HRS-06.1	Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both	5	
PS-06	Access Agreements	frequency]; andc. Verify that individuals requiring access to organizational information and systems:1. Sign appropriate access agreements prior to being granted access; and2. Re-sign access agreements to	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	

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
PS-07	External Personnel Security	by the organization;c. Document personnel security requirements;d. Require external providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of external personnel who possess organizational credentials	Functional	Equal	Third-Party Personnel	HRS-10	third-party personnel by reviewing and monitoring third-party security, compliance and/or resilience roles and	10	
PS-08	Personnel Sanctions	and privacy policies and procedures; andb. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated,	Functional	Equal	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	10	
PS-09	Position Descriptions	Incorporate security and privacy roles and responsibilities into organizational position descriptions.	Functional	Equal	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
RA-01	Policy and Procedures	executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;b. Designate an [Assignment: organization-defined	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	5	
RA-01	Policy and Procedures	Executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;b. Designate an [Assignment: organization-defined	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
RA-01	Policy and Procedures	executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;b. Designate an [Assignment: organization-defined	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient	5	
RA-02	Security Categorization	stores, and transmits;b. Document the security categorization results, including supporting rationale, in the security plan for the system; andc. Verify that the authorizing official or authorizing official designated representative reviews and approves the	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,	10	
RA-03	Risk Assessment	risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;c. Document risk assessment results in [Selection (one): security and privacy plans;	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	5	
RA-03	Risk Assessment	risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;c. Document risk assessment results in [Selection (one): security and privacy plans;	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from	5	
RA-03(01)	Risk Assessment | Supply Chain Risk Assessment	components, and system services; and2. Update the supply chain risk assessment [Assignment: organization-defined frequency], when there are significant changes to the relevant supply chain, or when changes to the system, environments of	Functional	Equal	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or	10	
RA-05	Vulnerability Monitoring and Scanning	improper configurations;2. Formatting checklists and test procedures; and3. Measuring vulnerability impact;c. Analyze vulnerability scan reports and results from vulnerability monitoring;d. Remediate legitimate	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications	5	
RA-05	Vulnerability Monitoring and Scanning	improper configurations;2. Formatting checklists and test procedures; and3. Measuring vulnerability impact;c. Analyze vulnerability scan reports and results from vulnerability monitoring;d. Remediate legitimate	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5	
RA-05(02)	Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanned	Update the system vulnerabilities to be scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported].	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5	
RA-05(04)	Vulnerability Monitoring and Scanning | Discoverable Information	Determine information about the system that is discoverable and take [Assignment: organization-defined corrective actions].	Functional	Equal	Acceptable Discoverable Information	VPM-06.8	Mechanisms exist to define what information is allowed to be discoverable by adversaries and take corrective actions to	10	
RA-05(05)	Vulnerability Monitoring and Scanning | Privileged Access	Implement privileged access authorization to [Assignment: organization-defined system components] for [Assignment: organization-defined vulnerability scanning activities].	Functional	Equal	Privileged Access	VPM-06.3	Mechanisms exist to implement privileged access authorization for selected vulnerability scanning activities.	10	
RA-05(11)	Vulnerability Monitoring and Scanning | Public Disclosure Program	Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.	Functional	Equal	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance	10	
RA-07	Risk Response	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.	Functional	Equal	Risk Response	RSK-06.1	were performed to remediate findings from security, compliance and/or resilience-related: (1) Assessments;	10	
RA-09	Criticality Analysis	identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle].	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications	5	
SA-01	Policy and Procedures	Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;b. Designate an [Assignment: organization-defined	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient	5	
SA-01	Policy and Procedures	regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;b. Designate an [Assignment: organization-defined	Functional	Subset Of	Technology Development & Acquisition	TDA-01	implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet	10	
SA-01	Policy and Procedures	regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;b. Designate an [Assignment: organization-defined	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	5	
SA-01	Policy and Procedures	regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;b. Designate an [Assignment: organization-defined	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
SA-02	Allocation of Resources	Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; andc. Establish a discrete	Functional	Equal	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection	10	
SA-03	System Development Life Cycle	security and privacy considerations;b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;c. Identify individuals having information security and privacy roles and responsibilities; andd.	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	security and privacy considerations;b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;c. Identify individuals having information security and privacy roles and responsibilities; andd.	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	5	
SA-04	Acquisition Process	requirements;c. Security and privacy assurance requirements;d. Controls needed to satisfy the security and privacy requirements.e. Security and privacy documentation requirements;f. Requirements for	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	5	
SA-04	Acquisition Process	requirements;c. Security and privacy assurance requirements;d. Controls needed to satisfy the security and privacy requirements.e. Security and privacy documentation requirements;f. Requirements for	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
SA-04	Acquisition Process	requirements;c. Security and privacy assurance requirements;d. Controls needed to satisfy the security and privacy requirements.e. Security and privacy documentation requirements;f. Requirements for	Functional	Intersects With	Technology Development & Acquisition	TDA-01	implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet	5	
SA-04	Acquisition Process	requirements;c. Security and privacy assurance requirements;d. Controls needed to satisfy the security and privacy requirements.e. Security and privacy documentation requirements;f. Requirements for	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,	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(01)	Acquisition Process | Functional Properties of Controls	Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.	Functional	Intersects With	Functional Properties	TDA-04.1	Mechanisms exist to require software developers to provide information describing the functional properties of the	5	
SA-04(01)	Acquisition Process | Functional Properties of Controls	Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	(1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network	5	
SA-04(02)	Acquisition Process | Design and Implementation Information for Controls	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	(1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network	5	
SA-04(02)	Acquisition Process | Design and Implementation Information for Controls	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and	Functional	Intersects With	Access to Program Source Code	TDA-20	Mechanisms exist to limit privileges to change software resident within software libraries.	5	
SA-04(02)	Acquisition Process | Design and Implementation Information for Controls	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and	Functional	Intersects With	Functional Properties	TDA-04.1	Mechanisms exist to require software developers to provide information describing the functional properties of the	5	
SA-04(05)	Acquisition Process | System, Component, and Service Configurations	Require the developer of the system, system component, or system service to: Deliver the system, component, or service with [Assignment: organization-defined security configurations] implemented; andb. Use the configurations as the default for any subsequent system, component, or service	Functional	Equal	Pre-Established Secure Configurations	TDA-02.4	Mechanisms exist to ensure vendors / manufacturers: (1) Deliver the Technology Asset, Application and/or Service (TAAS)	10	
SA-04(09)	Acquisition Process | Functions, Ports, Protocols, and Services in Use	Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.	Functional	Equal	Ports, Protocols & Services In Use	TDA-02.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to identify early in the	10	
SA-04(10)	Acquisition Process | Use of Approved PIV Products	Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.	Functional	Intersects With	Information Assurance Enabled Products	TDA-02.2	(IA-enabled) IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved	5	
SA-04(12)	Acquisition Process | Data Ownership	a. Include organizational data ownership requirements in the acquisition contract; andb. Require all data to be removed from the contractor's system and returned to the organization within [Assignment: organization-defined time frame].	Functional	Intersects With	Personal Data (PD) Lineage	PRI-09	Mechanisms exist to maintain a process to document the lineage of Personal Data (PD) by recording how the organization	5	
SA-04(12)	Acquisition Process | Data Ownership	a. Include organizational data ownership requirements in the acquisition contract; andb. Require all data to be removed from the contractor's system and returned to the organization within [Assignment: organization-defined time frame].	Functional	Intersects With	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	5	
SA-04(12)	Acquisition Process | Data Ownership	a. Include organizational data ownership requirements in the acquisition contract; andb. Require all data to be removed from the contractor's system and returned to the organization within [Assignment: organization-defined time frame].	Functional	Intersects With	Asset Ownership Assignment	AST-03	are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common	5	
SA-05	System Documentation	accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;2. Methods for user interaction, which enables individuals to use the system, component, or	Functional	Intersects With	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications	5	
SA-05	System Documentation	accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;2. Methods for user interaction, which enables individuals to use the system, component, or	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and	5	
SA-08	Security and Privacy Engineering Principles	engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications	5	
SA-08	Security and Privacy Engineering Principles	engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the	5	
SA-09	External System Services	[Assignment: organization-defined controls];b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; andc. Employ the following processes, methods, and techniques to monitor control	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,	10	
SA-09(02)	External System Services | Identification of Functions, Ports, Protocols, and	Require providers of [Assignment: organization-defined external system services] to identify the functions, ports, protocols, and other services required for the use of such services: [Assignment: organization-defined external system services]	Functional	Equal	Connectivity Requirements - Identification of Ports, Protocols &	TPM-04.2	Mechanisms exist to require External Service Providers (ESPs) to identify and document the business need for ports,	10	
SA-10	Developer Configuration Management	changes to [Assignment: organization-defined configuration items under configuration management];c. Implement only organization-approved changes to the system, component, or	Functional	Equal	Developer Configuration Management	TDA-14	system developers and integrators to perform configuration management during system design, development, implementation	10	
SA-11	Developer Testing and Evaluation	and privacy control assessments;d. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency] at [Assignment: organization-defined depth	Functional	Equal	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct	10	
SA-15	Development Process, Standards, and Tools	configurations used in the development process; and4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; andb. Review the development process, standards, tools, tool options, and tool configurations	Functional	Equal	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	
SA-15(03)	Development Process, Standards, and Tools | Criticality Analysis	analysis:a. At the following decision points in the system development life cycle: [Assignment: organization-defined decision points in the system development life cycle]; andb. At the following level of	Functional	Equal	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality	10	
SA-16	Developer-provided Training	component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: [Assignment: organization-defined	Functional	Equal	Developer-Provided Training	TDA-16	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to provide training on the	10	
SA-17	Developer Security and Privacy Architecture and Design	and privacy architecture that is an integral part the organization's enterprise architecture;b. Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; and	Functional	Equal	Developer Architecture & Design	TDA-05	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a design	10	
SA-21	Developer Screening	system service:a. Has appropriate access authorizations as determined by assigned [Assignment: organization-defined official government duties]; andb. Satisfies the following additional personnel screening criteria: [Assignment:	Functional	Equal	Developer Screening	TDA-13	Mechanisms exist to ensure that the developers of Technology Assets, Applications and/or Services (TAAS) have the	10	
SA-22	Unsupported System Components	components is no longer available from the developer, vendor, or manufacturer; orb. Provide the following options for alternative sources for continued support for unsupported components [Selection (one or more): in-house support; [Assignment: organization-defined	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:	5	
SA-22	Unsupported System Components	components is no longer available from the developer, vendor, or manufacturer; orb. Provide the following options for alternative sources for continued support for unsupported components [Selection (one or more): in-house support; [Assignment: organization-defined	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	5	
SC-01	Policy and Procedures	guidelines; and2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;b. Designate an	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient	5	
SC-01	Policy and Procedures	guidelines; and2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;b. Designate an	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
SC-01	Policy and Procedures	guidelines; and2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;b. Designate an	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the	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
SC-01	Policy and Procedures	guidelines; and2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;b. Designate an	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	5	
SC-02	Separation of System and User Functionality	Separate user functionality, including user interface services, from system management functionality.	Functional	Equal	Application Partitioning	SEA-03.2	Mechanisms exist to separate user functionality from system management functionality.	10	
SC-03	Security Function Isolation	Isolate security functions from nonsecurity functions.	Functional	Intersects With	Restrict Access To Security Functions	END-16	security functions are restricted to authorized individuals and enforce least privilege control requirements for necessary job	5	
SC-03	Security Function Isolation	Isolate security functions from nonsecurity functions.	Functional	Intersects With	Security Function Isolation	SEA-04.1	Mechanisms exist to isolate security functions from non-security functions.	5	
SC-04	Information in Shared System Resources	Prevent unauthorized and unintended information transfer via shared system resources.	Functional	Equal	Information In Shared Resources	SEA-05	Mechanisms exist to prevent unauthorized and unintended information transfer via shared system resources.	10	
SC-05	Denial-of-service Protection	the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]; andb. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are	5	
SC-05	Denial-of-service Protection	the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]; andb. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-	Functional	Intersects With	Capacity Planning	CAP-03	capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist	5	
SC-05	Denial-of-service Protection	the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]; andb. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-	Functional	Intersects With	Capacity & Performance Management	CAP-01	implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated	5	
SC-05	Denial-of-service Protection	the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]; andb. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-	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	subnetworks for publicly accessible system components that are [Selection (one): physically; logically] separated from internal organizational networks; andc. Connect to external networks or systems only through managed interfaces consisting of	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network	5	
SC-07(03)	Boundary Protection | Access Points	Limit the number of external network connections to the system.	Functional	Equal	Limit Network Connections	NET-03.1	Mechanisms exist to limit the number of concurrent external network connections to its Technology Assets, Applications	10	
SC-07(04)	Boundary Protection | External Telecommunications Services	mission or business need and duration of that need;e. Review exceptions to the traffic flow policy [Assignment: organization-defined frequency] and remove exceptions that are no longer supported by an explicit mission or business need;f. Prevent	Functional	Intersects With	External Telecommunications Services	NET-03.2	external telecommunication service that protects the confidentiality and integrity of the information being	5	
SC-07(05)	Boundary Protection | Deny by Default — Allow by Exception	Deny network communications traffic by default and allow network communications traffic by exception [Selection (one or more): at managed interfaces; for [Assignment: organization-defined systems]].	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit	5	
SC-07(07)	Boundary Protection | Split Tunneling for Remote Devices	Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using [Assignment: organization-defined safeguards].	Functional	Equal	Split Tunneling	CFG-03.4	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards	10	
SC-07(08)	Boundary Protection | Route Traffic to Authenticated Proxy Servers	Route [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.	Functional	Intersects With	Route Internal Traffic to Proxy Servers	NET-18.1	Mechanisms exist to route internal communications traffic to external networks through organization-approved proxy servers at managed interfaces	5	
SC-07(08)	Boundary Protection | Route Traffic to Authenticated Proxy Servers	Route [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.	Functional	Intersects With	DNS & Content Filtering	NET-18	through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to	5	
SC-07(18)	Boundary Protection | Fail Secure	Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the	5	
SC-07(21)	Boundary Protection | Isolation of System Components	Employ boundary protection mechanisms to isolate [Assignment: organization-defined system components] supporting [Assignment: organization-defined missions and/or business functions].	Functional	Equal	Isolation of System Components	NET-03.7	Mechanisms exist to employ boundary protections to isolate Technology Assets, Applications and/or Services (TAAS) that	10	
SC-07(28)	Boundary Protection | Connections to Public Networks	Prohibit the direct connection of [Assignment: organization-defined system] to a public network.	Functional	Equal	Direct Internet Access Restrictions	NET-06.5	Mechanisms exist to prohibit, or strictly-control, Internet access from sensitive/regulated data enclaves (secure zones).	10	
SC-07(29)	Boundary Protection | Separate Subnets to Isolate Functions	Implement [Selection (one): physically; logically] separate subnetworks to isolate the following critical system components and functions: [Assignment: organization-defined critical system components and functions]	Functional	Intersects With	Cloud Infrastructure Security Subnet	CLD-03	Mechanisms exist to host security-specific technologies in a dedicated subnet.	5	
SC-08	Transmission Confidentiality and Integrity	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
SC-08	Transmission Confidentiality and Integrity	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
SC-08(01)	Transmission Confidentiality and Integrity | Cryptographic Protection	Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	Functional	Intersects With	Alternate Physical Protection	CRY-01.1	Cryptographic mechanisms exist to prevent unauthorized disclosure of information as an alternative to physical safeguards	5	
SC-08(01)	Transmission Confidentiality and Integrity | Cryptographic Protection	Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies	5	
SC-08(01)	Transmission Confidentiality and Integrity | Cryptographic Protection	Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
SC-12	Cryptographic Key Establishment and Management	cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage,	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-12(01)	Cryptographic Key Establishment and Management | Availability	Maintain availability of information in the event of the loss of cryptographic keys by users.	Functional	Equal	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	10	
SC-13	Cryptographic Protection	cryptographic uses]; andb. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography for each specified cryptographic	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
SC-13	Cryptographic Protection	cryptographic uses]; andb. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography for each specified cryptographic	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	

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-13	Cryptographic Protection	cryptographic uses]; andb. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography for each specified cryptographic	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-15	Collaborative Computing Devices and Applications	computing devices and applications with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; andb. Provide an explicit indication of use to users	Functional	Intersects With	Collaborative Computing Devices	END-14	collaborative computing devices with the following exceptions: (1) Networked whiteboards; (2) Video teleconference	5	
SC-17	Public Key Infrastructure Certificates	organization-defined certificate policy] or obtain public key certificates from an approved service provider; andb. Include only approved trust anchors in trust stores or certificate stores managed by the	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	a. Define acceptable and unacceptable mobile code and mobile code technologies; andb. Authorize, monitor, and control the use of mobile code within the system.	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
SC-20	Secure Name/address Resolution Service (authoritative Source)	in response to external name/address resolution queries; andb. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a	Functional	Intersects With	Domain Name Service (DNS) Resolution	NET-10	Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name /	5	
SC-21	Name/address Resolution Service (recursive or Caching Resolver)	Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.	Functional	Equal	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	NET-10.2	data origin authentication and data integrity verification on the Domain Name Service (DNS) resolution responses received from authoritative sources when	10	
SC-22	Architecture and Provisioning for Name/address Resolution Service	Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.	Functional	Equal	Architecture & Provisioning for Name / Address Resolution Service	NET-10.1	systems that collectively provide Domain Name Service (DNS) resolution service are fault-tolerant and implement	10	
SC-23	Session Authenticity	Protect the authenticity of communications sessions.	Functional	Equal	Session Integrity	NET-09	Mechanisms exist to protect the authenticity and integrity of communications sessions.	10	
SC-24	Fail in Known State	system state] for the following failures on the indicated components while preserving [Assignment: organization-defined system state information] in failure: [Assignment: list of organization-defined types of system failures on organization-defined system	Functional	Intersects With	Fail Secure	SEA-07.2	systems to fail to an organization-defined known-state for types of failures, preserving system state information in	5	
SC-28	Protection of Information at Rest	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	
SC-28	Protection of Information at Rest	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
SC-28(01)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5	
SC-28(01)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
SC-28(01)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
SC-28(01)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]	Functional	Intersects With	Encrypting Data In Storage Media	DCH-07.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	5	
SC-39	Process Isolation	Maintain a separate execution domain for each executing system process.	Functional	Equal	Process Isolation	SEA-04	Mechanisms exist to implement a separate execution domain for each executing process.	10	
SC-41	Port and I/O Device Access	[Selection (one): Physically; Logically] disable or remove [Assignment: organization-defined connection ports or input/output devices] on the following systems or system components: [Assignment: organization-defined systems or system components]	Functional	Equal	Port & Input / Output (I/O) Device Access	END-12	Mechanisms exist to physically disable or remove unnecessary connection ports or input/output devices from sensitive systems.	10	
SC-45	System Time Synchronization	Synchronize system clocks within and between systems and system components.	Functional	Intersects With	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	5	
SC-47	Alternate Communications Channels	Establish [Assignment: organization-defined alternate communications paths] for system operations organizational command and control.	Functional	Equal	Alternate Communications Channels	BCD-10.4	command and control capabilities via alternate communications channels and designating alternative decision makers if primary decision	10	
SI-01	Policy and Procedures	regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;b. Designate an [Assignment: organization-defined	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	5	
SI-01	Policy and Procedures	regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;b. Designate an [Assignment: organization-defined	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the	10	
SI-01	Policy and Procedures	regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;b. Designate an [Assignment: organization-defined	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient	5	
SI-02	Flaw Remediation	remediation for effectiveness and potential side effects before installation;c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
SI-02	Flaw Remediation	remediation for effectiveness and potential side effects before installation;c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services	5	
SI-02	Flaw Remediation	remediation for effectiveness and potential side effects before installation;c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5	
SI-02(02)	Flaw Remediation | Automated Flaw Remediation Status	Determine if system components have applicable security-relevant software and firmware updates installed using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]	Functional	Intersects With	Automated Remediation Status	VPM-05.2	Automated mechanisms exist to determine the state of system components with regard to flaw remediation.	5	
SI-03	Malicious Code Protection	organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services	5	
SI-03	Malicious Code Protection	organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
SI-03	Malicious Code Protection	organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
SI-03	Malicious Code Protection	organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance	Functional	Intersects With	Heuristic / Nonsignature-Based Detection	END-04.4	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	5	
SI-03	Malicious Code Protection	organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public	5	
SI-03	Malicious Code Protection	organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5	
SI-03	Malicious Code Protection	organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
SI-04	System Monitoring	deploy monitoring devices:1. Strategically within the system to collect organization-determined essential information; and2. At ad hoc locations within the system to track specific types of transactions of interest to the organization:d. Analyze detected events	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
SI-04	System Monitoring	deploy monitoring devices:1. Strategically within the system to collect organization-determined essential information; and2. At ad hoc locations within the system to track specific types of transactions of interest to the organization:d. Analyze detected events	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related	5	
SI-04	System Monitoring	deploy monitoring devices:1. Strategically within the system to collect organization-determined essential information; and2. At ad hoc locations within the system to track specific types of transactions of interest to the organization:d. Analyze detected events	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public	5	
SI-04	System Monitoring	deploy monitoring devices:1. Strategically within the system to collect organization-determined essential information; and2. At ad hoc locations within the system to track specific types of transactions of interest to the organization:d. Analyze detected events	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
SI-04(02)	System Monitoring | Automated Tools and Mechanisms for Real-time Analysis	Employ automated tools and mechanisms to support near real-time analysis of events.	Functional	Equal	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation	10	
SI-04(04)	System Monitoring | Inbound and Outbound Communications Traffic	activities or conditions for inbound and outbound communications traffic;b. Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized	Functional	Equal	Inbound & Outbound Communications Traffic	MON-01.3	continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or	10	
SI-04(05)	System Monitoring | System-generated Alerts	roles] when the following system-generated indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators]	Functional	Equal	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection	10	
SI-04(10)	System Monitoring | Visibility of Encrypted Communications	Make provisions so that [Assignment: organization-defined encrypted communications traffic] is visible to [Assignment: organization-defined system monitoring tools and mechanisms].	Functional	Equal	Visibility of Encrypted Communications	NET-18.2	Mechanisms exist to configure the proxy to make encrypted communications traffic visible to monitoring tools and mechanisms.	10	
SI-04(12)	System Monitoring | Automated Organization-generated Alerts	roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [Assignment:	Functional	Intersects With	Automated Alerts	MON-01.12	automatically alert incident response personnel to inappropriate or anomalous activities that have potential	5	
SI-04(14)	System Monitoring | Wireless Intrusion Detection	Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.	Functional	Intersects With	Wireless Network Monitoring	MON-01.5	Mechanisms exist to monitor wireless network segments for: (1) Rogue wireless devices; and (2) Anomalous and/or hostile activities	5	
SI-04(20)	System Monitoring | Privileged Users	Implement the following additional monitoring of privileged users: [Assignment: organization-defined additional monitoring].	Functional	Equal	Privileged User Oversight	MON-01.15	Mechanisms exist to implement enhanced activity monitoring for privileged users.	10	
SI-04(22)	System Monitoring | Unauthorized Network Services	authorized or approved by [Assignment: organization-defined authorization or approval processes]; andb. [Selection (one or more): Audit; Alert [Assignment: organization-defined personnel or roles]] when	Functional	Equal	Unauthorized Network Services	MON-11.2	Automated mechanisms exist to detect unauthorized network services and alert incident response personnel.	10	
SI-05	Security Alerts, Advisories, and Directives	directives as deemed necessary;c. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment:	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	directives as deemed necessary;c. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment:	Functional	Intersects With	Threat Intelligence Feeds	THR-03	vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of	5	
SI-05	Security Alerts, Advisories, and Directives	directives as deemed necessary;c. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment:	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public	5	
SI-06	Security and Privacy Function Verification	organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]];c. Alert [Assignment: organization-defined personnel or roles]	Functional	Intersects With	Control Functionality Verification	CHG-06	functionality of security, compliance and resilience controls following implemented changes to ensure applicable	5	
SI-07	Software, Firmware, and Information Integrity	unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; andb. Take the following actions when unauthorized changes to the software, firmware, and information are	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-06	Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and	5	
SI-07	Software, Firmware, and Information Integrity	unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; andb. Take the following actions when unauthorized changes to the software, firmware, and information are	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public	5	
SI-07	Software, Firmware, and Information Integrity	unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; andb. Take the following actions when unauthorized changes to the software, firmware, and information are	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	organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment:	Functional	Equal	Integrity Checks	END-06.1	Mechanisms exist to validate configurations through integrity checking of software and firmware.	10	
SI-07(02)	and Information Integrity | Automated Notifications of	Employ automated tools that provide notification to [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification.	Functional	Equal	Automated Notifications of Integrity Violations	END-06.3	Automated mechanisms exist to alert incident response personnel upon discovering discrepancies during integrity verification.	10	
SI-07(05)	and Information Integrity | Automated Response to	Automatically [Selection (one or more): shut the system down; restart the system; implement [Assignment: organization-defined controls]] when integrity violations are discovered.	Functional	Equal	Automated Response to Integrity Violations	END-06.4	Automated mechanisms exist to implement remediation actions when integrity violations are discovered.	10	
SI-07(07)	and Information Integrity | Integration of Detection and	Incorporate the detection of the following unauthorized changes into the organizational incident response capability: [Assignment: organization-defined security-relevant changes to the system].	Functional	Equal	Endpoint Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.	10	
SI-07(15)	Software, Firmware, and Information Integrity | Code Authentication	Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: [Assignment: organization-defined software or firmware components].	Functional	Intersects With	Signed Components	CHG-04.2	installation of software and firmware components without verification that the component has been digitally signed using	5	
SI-08	Spam Protection	entry and exit points to detect and act on unsolicited messages; andb. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and	Functional	Equal	Phishing & Spam Protection	END-08	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail	10	

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-10	Information Input Validation	Check the validity of the following information inputs: [Assignment: organization-defined information inputs to the system].	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public	5	
SI-10	Information Input Validation	Check the validity of the following information inputs: [Assignment: organization-defined information inputs to the system].	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
SI-11	Error Handling	a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; andb. Reveal error messages only to [Assignment: organization-defined personnel or roles]	Functional	Equal	Error Handling	TDA-19	(2) Generating error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in	10	
SI-12	Information Management and Retention	Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
SI-12	Information Management and Retention	Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period	5	
SI-13	Predictable Failure Prevention	of operation: [Assignment: organization-defined system components]; andb. Provide substitute system components and a means to exchange active and standby components in accordance with the following	Functional	Intersects With	Failover Capability	BCD-12.2	Mechanisms exist to implement real-time or near-real-time failover capability to maintain availability of critical Technology	5	
SI-13	Predictable Failure Prevention	of operation: [Assignment: organization-defined system components]; andb. Provide substitute system components and a means to exchange active and standby components in accordance with the following	Functional	Intersects With	Predictable Failure Analysis	SEA-07	Mechanisms exist to determine the Mean Time to Failure (MTTF) for system components in specific environments of operation.	5	
SI-16	Memory Protection	Implement the following controls to protect the system memory from unauthorized code execution: [Assignment: organization-defined controls].	Functional	Equal	Memory Protection	SEA-10	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	10	
SI-17	Fail-safe Procedures	Implement the indicated fail-safe procedures when the indicated failures occur: [Assignment: organization-defined list of failure conditions and associated fail-safe procedures].	Functional	Equal	Fail Safe	SEA-07.3	Mechanisms exist to implement fail-safe procedures when failure conditions occur.	10	
SR-01	Policy and Procedures	regulations, policies, standards, and guidelines; andz. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;b. Designate an [Assignment: organization-defined	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	5	
SR-01	Policy and Procedures	regulations, policies, standards, and guidelines; andz. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;b. Designate an [Assignment: organization-defined	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient	5	
SR-01	Policy and Procedures	regulations, policies, standards, and guidelines; andz. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;b. Designate an [Assignment: organization-defined	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
SR-02	Supply Chain Risk Management Plan	services: [Assignment: organization-defined systems, system components, or system services];b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency] or as	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development,	5	
SR-02	Supply Chain Risk Management Plan	following systems, system components or system services: [Assignment: organization-defined systems, system components, or system services];b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency] or as	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications	5	
SR-02(01)	Supply Chain Risk Management Plan | Establish SCRM Team	consisting of [Assignment: organization-defined personnel, roles, and responsibilities] to lead and support the following SCRM activities: [Assignment: organization-defined supply chain risk management	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications	5	
SR-03	Supply Chain Controls and Processes	personnel];b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined supply chain	Functional	Equal	Processes To Address Weaknesses or Deficiencies	TPM-03.3	Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain	10	
SR-05	Acquisition Strategies, Tools, and Methods	Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined acquisition strategies, contract tools, and procurement methods].	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of	5	
SR-05(01)	Acquisition Strategies, Tools, and Methods | Adequate Supply	Employ the following controls to ensure an adequate supply of [Assignment: organization-defined critical system components]: [Assignment: organization-defined controls].	Functional	Equal	Adequate Supply	TPM-03.4	implement a spare parts strategy to ensure that an adequate supply of critical components is available to meet operational	10	
SR-06	Supplier Assessments and Reviews	Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [Assignment: organization-defined frequency].	Functional	Intersects With	Review of Third-Party Services	TPM-08	regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and	5	
SR-08	Notification Agreements	involved in the supply chain for the system, system component, or system service for the [Selection (one or more): notification of supply chain compromises; results of assessments or audits; [Assignment:	Functional	Equal	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the	10	
SR-09	Tamper Resistance and Detection	Implement a tamper protection program for the system, system component, or system service.	Functional	Intersects With	Logical Tampering Protection	AST-15	Mechanisms exist to assess the integrity of critical Technology Assets, Applications and/or Services (TAAS) to detect	5	
SR-09(01)	and Detection | Multiple Stages of System Development Life	Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle.	Functional	Intersects With	Logical Tampering Protection	AST-15	Mechanisms exist to assess the integrity of critical Technology Assets, Applications and/or Services (TAAS) to detect	5	
SR-10	Inspection of Systems or Components	[Selection (one or more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering: [Assignment:	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means	5	
SR-10	Inspection of Systems or Components	[Selection (one or more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering: [Assignment:	Functional	Intersects With	Technology Asset Inspections	AST-15.1	Mechanisms exist to physically and logically inspect critical technology assets to detect evidence of tampering.	5	
SR-11	Component Authenticity	prevent counterfeit components from entering the system; andb. Report counterfeit system components to [Selection (one or more): source of counterfeit component; [Assignment: organization-defined	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means	5	
SR-11(01)	Component Authenticity | Anti-counterfeit Training	Train [Assignment: organization-defined personnel or roles] to detect counterfeit system components (including hardware, software, and firmware).	Functional	Equal	Anti-Counterfeit Training	TDA-11.1	Mechanisms exist to train personnel to detect counterfeit system components, including hardware, software and firmware.	10	
SR-11(02)	Authenticity | Configuration Control for Component Service	Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: [Assignment: organization-defined system components]	Functional	Equal	Maintain Configuration Control During Maintenance	MNT-07	Mechanisms exist to maintain proper physical security and configuration control over technology assets awaiting service or repair.	10	
SR-12	Component Disposal	Dispose of [Assignment: organization-defined data, documentation, tools, or system components] using the following techniques and methods: [Assignment: organization-defined techniques and methods].	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered	5	