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
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-r3.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-82 Low Overlay
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
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
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-01
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
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
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
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
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(06)	Account Management | Dynamic Privilege Management	Implement [Assignment: organization-defined dynamic privilege management capabilities].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-02(07)	Account Management | Privileged User Accounts	accordance with [Selection (one): a role-based access scheme; an attribute-based access scheme];b. Monitor privileged role or attribute assignments;c. Monitor changes to roles or attributes; andd. Revoke access when privileged role or attribute assignments are no	Functional	Equal	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or	10		
AC-02(08)	Account Management | Dynamic Account Management	Create, activate, manage, and deactivate [Assignment: organization-defined system accounts] dynamically.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-02(09)	Account Management | Restrictions on Use of Shared and Group Accounts	Only permit the use of shared and group accounts that meet [Assignment: organization-defined conditions for establishing shared and group accounts].	Functional	Equal	Restrictions on Shared Groups / Accounts	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	10		
AC-02(10)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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
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
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
AC-03(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
AC-03(02)	Access Enforcement | Dual Authorization	Enforce dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined actions].	Functional	Intersects With	Two-Person Rule	HRS-12.1	Mechanisms exist to enforce a two-person rule for implementing changes to sensitive Technology Assets, Applications and/or	5		
AC-03(02)	Access Enforcement | Dual Authorization	Enforce dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined actions].	Functional	Intersects With	Dual Authorization for Privileged Commands	IAC-20.5	Automated mechanisms exist to enforce dual authorization for privileged commands.	5		
AC-03(03)	Access Enforcement | Mandatory Access Control	subjects or objects;2. Granting its privileges to other subjects;3. Changing one or more security attributes (specified by the policy) on subjects, objects, the system, or system components;4. Choosing the	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-03(04)	Access Enforcement | Discretionary Access Control	been granted access to information can do one or more of the following:a. Pass the information to any other subjects or objects;b. Grant its privileges to other subjects;c. Change security attributes on subjects,	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-03(05)	Access Enforcement | Security-relevant Information	Prevent access to [Assignment: organization-defined security-relevant information] except during secure, non-operable system states.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-03(06)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
AC-03(07)	Access Enforcement | Role-based Access Control	Enforce a role-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined roles and users authorized to assume such roles].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	

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	NIST SP 800-82 Low Overlay
AC-03(08)	Access Enforcement | Revocation of Access Authorizations	Enforce the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on [Assignment: organization-defined rules governing the timing of revocations of access authorizations].	Functional	Equal	Revocation of Access Authorizations	IAC-20.6	Mechanisms exist to revoke logical and physical access authorizations.	10		
AC-03(09)	Access Enforcement | Controlled Release	Before releasing information to external [Assignment: organization-defined system or system component] provides [Assignment: organization-defined controls]; andb. [Assignment: organization-defined controls] are used to validate the appropriateness of the information designated for	Functional	Equal	Controlled Release	DCH-03.3	Automated mechanisms exist to validate cybersecurity and data protection attributes prior to releasing information to external	10		
AC-03(10)	Access Enforcement | Audited Override of Access Control Mechanisms	Employ an audited override of automated access control mechanisms under [Assignment: organization-defined conditions] by [Assignment: organization-defined roles].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-03(11)	Access Enforcement | Restrict Access to Specific Information Types	Restrict access to data repositories containing [Assignment: organization-defined information types].	Functional	Equal	Sensitive / Regulated Data Access Enforcement	CFG-08	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to restrict access to sensitive/regulated	10		
AC-03(12)	Access Enforcement | Assert and Enforce Application Access	During application installation process, the access needed to the following system applications and functions: [Assignment: organization-defined system applications and functions];b. Provide an enforcement mechanism to prevent unauthorized access; andc. Approve access	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-03(13)	Access Enforcement | Attribute-based Access Control	Enforce attribute-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined attributes to assume access permissions].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-03(14)	Access Enforcement | Individual Access	Provide [Assignment: organization-defined mechanisms] to enable individuals to have access to the following elements of their personally identifiable information: [Assignment: organization-defined elements].	Functional	Equal	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data	10		
AC-03(15)	Access Enforcement | Discretionary and Mandatory Access Control	Enforce [Assignment: organization-defined mandatory access control policy] over the set of covered subjects and objects specified in the policy; andb. Enforce [Assignment: organization-defined discretionary access control policy] over the set of	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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(01)	Information Flow Enforcement | Object Security and Privacy Attributes	Use [Assignment: organization-defined security and privacy attributes] associated with [Assignment: organization-defined information, source, and destination objects] to enforce [Assignment: organization-defined information flow control policies]	Functional	Equal	Object Security Attributes	NET-04.2	security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow	10		
AC-04(02)	Information Flow Enforcement | Processing Domains	Use protected processing domains to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-04(03)	Information Flow Enforcement | Dynamic Information Flow Control	Enforce [Assignment: organization-defined information flow control policies].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-04(04)	Information Flow Enforcement | Flow Control of Encrypted Information	Prevent encrypted information from bypassing [Assignment: organization-defined flow control mechanisms] by [Selection (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information;	Functional	Equal	Content Check for Encrypted Data	NET-04.3	Mechanisms exist to prevent encrypted data from bypassing content-checking mechanisms.	10		
AC-04(05)	Information Flow Enforcement | Embedded Data Types	Enforce [Assignment: organization-defined limitations] on embedding data types within other data types.	Functional	Equal	Embedded Data Types	NET-04.4	Mechanisms exist to enforce limitations on embedding data within other data types.	10		
AC-04(06)	Information Flow Enforcement | Metadata	Enforce information flow control based on [Assignment: organization-defined metadata].	Functional	Equal	Metadata	NET-04.5	Mechanisms exist to enforce information flow controls based on metadata.	10		
AC-04(07)	Information Flow Enforcement | One-way Flow Mechanisms	Enforce one-way information flows through hardware-based flow control mechanisms.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-04(08)	Information Flow Enforcement | Security and Privacy Policy Filters	[Assignment: organization-defined security or privacy policy filters] as a basis for flow control decisions for [Assignment: organization-defined information flows]; andb. [Selection (one or more): Block; Strip; Modify; Quarantine] data after a filter processing failure in	Functional	Equal	Policy Decision Point (PDP)	NET-04.7	evaluate access requests against established criteria to dynamically and uniformly enforce access rights and	10		
AC-04(09)	Information Flow Enforcement | Human Reviews	Enforce the use of human reviews for [Assignment: organization-defined information flows] under the following conditions: [Assignment: organization-defined conditions].	Functional	Equal	Human Reviews	NET-04.6	Mechanisms exist to enforce the use of human reviews for Access Control Lists (ACLs) and similar rulesets on a routine basis.	10		
AC-04(10)	Information Flow Enforcement | Enable and Disable Security or Privacy Policy Filters	Provide the capability for privileged administrators to enable and disable [Assignment: organization-defined security or privacy policy filters] under the following conditions: [Assignment: organization-defined conditions]	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-04(11)	Information Flow Enforcement | Configuration of Security or Privacy Policy Filters	Provide the capability for privileged administrators to configure [Assignment: organization-defined security or privacy policy filters] to support different security or privacy policies.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-04(12)	Information Flow Enforcement | Data Type Identifiers	When transferring information between different security domains, use [Assignment: organization-defined data type identifiers] to validate data essential for information flow decisions.	Functional	Equal	Data Type Identifiers	NET-04.8	utilize data type identifiers to validate data essential for information flow decisions when transferring information between	10		
AC-04(13)	Information Flow Enforcement | Decomposition into Policy-relevant Subcomponents	When transferring information between different security domains, decompose information into [Assignment: organization-defined policy-relevant subcomponents] for submission to policy enforcement mechanisms.	Functional	Equal	Decomposition Into Policy-Related Subcomponents	NET-04.9	decompose information into policy-relevant subcomponents for submission to policy enforcement mechanisms, when transferring information between	10		
AC-04(14)	Information Flow Enforcement | Security or Privacy Policy Filter Constraints	When transferring information between different security domains, implement [Assignment: organization-defined security or privacy policy filters] requiring fully enumerated formats that restrict data structure and content	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-04(15)	Information Flow Enforcement | Detection of Unsanctioned Information	When transferring information between different security domains, examine the information for the presence of [Assignment: organization-defined unsanctioned information] and prohibit the transfer of such information in accordance with the [Assignment:	Functional	Equal	Detection of Unsanctioned Information	NET-04.10	implement security policy filters requiring fully enumerated formats that restrict data structure and content, when transferring information between	10		
AC-04(16)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
AC-04(17)	Information Flow Enforcement | Domain Authentication	Uniquely identify and authenticate source and destination points by [Selection (one or more): organization; system; application; service; individual] for information transfer.	Functional	Equal	Cross Domain Authentication	NET-04.12	Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer	10		
AC-04(18)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
AC-04(19)	Information Flow Enforcement | Validation of Metadata	When transferring information between different security domains, implement [Assignment: organization-defined security or privacy policy filters] on metadata.	Functional	Equal	Metadata Validation	NET-04.13	Automated mechanisms exist to apply cybersecurity and/or data protection filters on metadata.	10		
AC-04(20)	Information Flow Enforcement | Approved Solutions	Employ [Assignment: organization-defined solutions in approved configurations] to control the flow of [Assignment: organization-defined information] across security domains.	Functional	Equal	Approved Solutions	NET-04.11	presence of unsanctioned information and prohibits the transfer of such information, when transferring information	10		
AC-04(21)	Information Flow Enforcement | Physical or Logical Separation of Information Flows	Separate information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization-defined required separations by types of information].	Functional	Equal	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications	10		
AC-04(22)	Information Flow Enforcement | Access Only	Provide access from a single device to computing platforms, applications, or data residing in multiple different security domains, while preventing information flow between the different security domains	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-04(23)	Information Flow Enforcement | Modify Non-releasable Information	When transferring information between different security domains, modify non-releasable information by implementing [Assignment: organization-defined modification action].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-82 Low Overlay
AC-04(24)	Information Flow Enforcement | Internal Normalized Format	When transferring information between different security domains, parse incoming data into an internal normalized format and regenerate the data to be consistent with its intended specification.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-04(25)	Information Flow Enforcement | Data Sanitization	When transferring information between different security domains, sanitize data to minimize [Selection (one or more): delivery of malicious content, command and control of malicious code, malicious code augmentation, and steganography encoded data; spillage of sensitive information] in accordance with	Functional	Equal	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period	10		
AC-04(26)	Information Flow Enforcement | Audit Filtering Actions	When transferring information between different security domains, record and audit content filtering actions and results for the information being filtered.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-04(27)	Information Flow Enforcement | Redundant/independent Filtering Mechanisms	When transferring information between different security domains, implement content filtering solutions that provide redundant and independent filtering mechanisms for each data type.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-04(28)	Information Flow Enforcement | Linear Filter Pipelines	When transferring information between different security domains, implement a linear content filter pipeline that is enforced with discretionary and mandatory access controls.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-04(29)	Information Flow Enforcement | Filter Orchestration Engines	security domains, employ content filter orchestration engines to ensure that:a. Content filtering mechanisms successfully complete execution without errors; andb. Content filtering actions occur in the correct order and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-04(30)	Information Flow Enforcement | Filter Mechanisms Using Multiple Processes	When transferring information between different security domains, implement content filtering mechanisms using multiple processes.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-04(31)	Information Flow Enforcement | Failed Content Transfer Prevention	When transferring information between different security domains, prevent the transfer of failed content to the receiving domain.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-04(32)	Enforcement | Process Requirements for Information	security domains, the process that transfers information between filter pipelines:a. Does not filter message content;b. Validates filtering metadata;c. Ensures the content associated with the filtering metadata has successfully completed filtering; andd.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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		
AC-06(01)	Least Privilege | Authorize Access to Security Functions	Authorize access for [Assignment: organization-defined individuals or roles] to:a. [Assignment: organization-defined security functions (deployed in hardware, software, and firmware)]; andb. [Assignment: organization-defined security-relevant information].	Functional	Equal	Authorize Access to Security Functions	IAC-21.1	Mechanisms exist to limit access to security functions to explicitly-authorized privileged users.	10		
AC-06(02)	Least Privilege | Non-privileged Access for Nonsecurity Functions	Require that users of system accounts (or roles) with access to [Assignment: organization-defined security functions or security-relevant information] use non-privileged accounts or roles, when accessing nonsecurity functions.	Functional	Equal	Non-Privileged Access for Non-Security Functions	IAC-21.2	Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.	10		
AC-06(03)	Least Privilege | Network Access to Privileged Commands	Authorize network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and document the rationale for such access in the security plan for the system.	Functional	Equal	Network Access to Privileged Commands	IAC-21.6	Mechanisms exist to authorize remote access to perform privileged commands on critical Technology Assets, Applications	10		
AC-06(04)	Least Privilege | Separate Processing Domains	Provide separate processing domains to enable finer-grained allocation of user privileges.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-06(05)	Least Privilege | Privileged Accounts	Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].	Functional	Equal	Management Approval For Privileged Accounts	IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles.	10		
AC-06(06)	Least Privilege | Privileged Access by Non-organizational Users	Prohibit privileged access to the system by non-organizational users.	Functional	Equal	Privileged Access by Non-Organizational Users	IAC-05.2	Mechanisms exist to prohibit privileged access by non-organizational users.	10		
AC-06(07)	Least Privilege | Review of User Privileges	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(08)	Least Privilege | Privilege Levels for Code Execution	Prevent the following software from executing at higher privilege levels than users executing the software: [Assignment: organization-defined software].	Functional	Equal	Privilege Levels for Code Execution	IAC-21.7	Automated mechanisms exist to prevent applications from executing at higher privilege levels than the user's privileges.	10		
AC-06(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-07
AC-07(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
AC-07(02)	Unsuccessful Logon Attempts | Purge or Wipe Mobile Device	organization-defined mobile devices] based on [Assignment: organization-defined purging or wiping requirements and techniques] after [Assignment: organization-defined number] consecutive,	Functional	Equal	Remote Purging	MDM-05	Mechanisms exist to remotely purge selected information from mobile devices.	10		
AC-07(03)	Unsuccessful Logon Attempts | Biometric Attempt Limiting	Limit the number of unsuccessful biometric logon attempts to [Assignment: organization-defined number].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-07(04)	Unsuccessful Logon Attempts | Use of Alternate Authentication Factor	primary authentication factors after the number of organization-defined consecutive invalid logon attempts have been exceeded; andb. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts through use of the	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-08	System Use Notification	subject to criminal and civil penalties; andb. 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-08

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	NIST SP 800-82 Low Overlay
AC-09	Previous Logon Notification	Notify the user, upon successful logon to the system, of the date and time of the last logon.	Functional	Equal	Previous Logon Notification	SEA-19	systems that process, store or transmit sensitive/regulated data to notify the user, upon successful logon, of the number of unsuccessful logon attempts	10		
AC-09(01)	Previous Logon Notification | Unsuccessful Logons	Notify the user, upon successful logon, of the number of unsuccessful logon attempts since the last successful logon.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-09(02)	Previous Logon Notification | Successful and Unsuccessful Logons	Notify the user, upon successful logon, of the number of [Selection (one): successful logons; unsuccessful logon attempts; both] during [Assignment: organization-defined time period].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-09(03)	Previous Logon Notification | Notification of Account Changes	Notify the user, upon successful logon, of changes to [Assignment: organization-defined security-related characteristics or parameters of the user's account] during [Assignment: organization-defined time period].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-09(04)	Previous Logon Notification | Additional Logon Information	Notify the user, upon successful logon, of the following additional information: [Assignment: organization-defined additional information].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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	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-12(01)	Session Termination | User-initiated Logouts	Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [Assignment: organization-defined information resources].	Functional	Equal	User-Initiated Logouts / Message Displays	IAC-25.1	Mechanisms exist to provide a logout capability and display an explicit logout message to users indicating the reliable termination of the session.	10		
AC-12(02)	Session Termination | Termination Message	Display an explicit logout message to users indicating the termination of authenticated communications sessions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-12(03)	Session Termination | Timeout Warning Message	Display an explicit message to users indicating that the session will end in [Assignment: organization-defined time until end of session].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-13		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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-14
AC-14(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
AC-15		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
AC-16	Security and Privacy Attributes	permitted security and privacy attributes from the attributes defined in AC-16a for [Assignment: organization-defined systems]: [Assignment: organization-defined security and privacy attributes];d. Determine the following permitted attribute values or	Functional	Equal	Cybersecurity & Data Protection Attributes	DCH-05	Mechanisms exist to bind cybersecurity and data protection attributes to information as it is stored, transmitted and processed.	10		
AC-16(01)	Security and Privacy Attributes | Dynamic Attribute Association	with [Assignment: organization-defined subjects and objects] in accordance with the following security and privacy policies as information is created and combined: [Assignment: organization-defined security	Functional	Equal	Dynamic Attribute Association	DCH-05.1	individuals and objects as information is created, combined, or transformed, in accordance with organization-	10		
AC-16(02)	Privacy Attributes | Attribute Value Changes by Authorized	Provide authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated security and privacy attributes.	Functional	Equal	Attribute Value Changes By Authorized Individuals	DCH-05.2	authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated	10		
AC-16(03)	Privacy Attributes | Maintenance of Attribute Associations by	Maintain the association and integrity of [Assignment: organization-defined security and privacy attributes] to [Assignment: organization-defined subjects and objects].	Functional	Equal	Maintenance of Attribute Associations By System	DCH-05.3	Mechanisms exist to maintain the association and integrity of cybersecurity and data protection attributes to individuals and objects	10		
AC-16(04)	Privacy Attributes | Association of Attributes by Authorized	Provide the capability to associate [Assignment: organization-defined security and privacy attributes] with [Assignment: organization-defined subjects and objects] by authorized individuals (or processes acting on behalf of individuals).	Functional	Equal	Association of Attributes By Authorized Individuals	DCH-05.4	cybersecurity and data protection attributes with individuals and objects by authorized individuals (or	10		
AC-16(05)	Privacy Attributes | Attribute Displays on Objects to Be Output	Display to [Assignment: organization-defined individuals assigned roles or classifications] [Assignment: organization-defined security and privacy attributes] in human-readable, standard	Functional	Equal	Attribute Displays for Output Devices	DCH-05.5	readable form on each object that the system transmits to output devices to identify special dissemination, handling or	10		
AC-16(06)	Privacy Attributes | Maintenance of Attribute Association	Require that the system transmits to output devices to identify [Assignment: organization-defined special dissemination, handling, or distribution instructions] using [Assignment: organization-defined human-readable, standard	Functional	Equal	Data Subject Attribute Associations	DCH-05.6	association of [Assignment: organization-defined security and privacy attributes] with [Assignment: organization-defined subjects and objects] in accordance with [Assignment: organization-defined	10		
AC-16(07)	Privacy Attributes | Consistent Attribute Interpretation	Provide a consistent interpretation of security and privacy attributes transmitted between distributed system components.	Functional	Equal	Consistent Attribute Interpretation	DCH-05.7	maintain the association of cybersecurity and data protection attributes with individuals and objects in	10		
AC-16(08)	Privacy Attributes | Association Techniques and Technologies	Implement [Assignment: organization-defined techniques and technologies] in associating security and privacy attributes to information.	Functional	Equal	Identity Association Techniques & Technologies	DCH-05.8	agreed upon interpretation of cybersecurity and data protection attributes employed in access enforcement and flow	10		
AC-16(09)	Privacy Attributes | Attribute Reassignment — Regrading	Change security and privacy attributes associated with information only via regrading mechanisms validated using [Assignment: organization-defined techniques or procedures].	Functional	Equal	Attribute Reassignment	DCH-05.9	Mechanisms exist to associate cybersecurity and data protection attributes to information.	10		
AC-16(10)	Privacy Attributes | Attribute Configuration by Authorized	Provide authorized individuals the capability to define or change the type and value of security and privacy attributes available for association with subjects and objects.	Functional	Equal	Attribute Configuration By Authorized Individuals	DCH-05.10	Mechanisms exist to reclassify data as required, due to changing business/technical requirements.	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	capability to define or change the type and value of cybersecurity and data protection attributes available for	10		
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	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5		AC-17
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	Automated mechanisms exist to monitor and control remote access sessions.	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	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).	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	Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).	10		
AC-17(05)		Withdrawn	Functional	No Relationship	N/A	N/A	execution of privileged commands and access to security-relevant information via remote access only for	0		Withdrawn
AC-17(06)	Remote Access | Protection of Mechanism Information	Protect information about remote access mechanisms from unauthorized use and disclosure.	Functional	Intersects With	Remote Access	NET-14	N/A	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	NIST SP 800-82 Low Overlay
AC-17(07)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
AC-17(08)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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(09)
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
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
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(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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
AC-19(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
AC-19(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
AC-19(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
AC-19(04)	Access Control for Mobile Devices | Restrictions for Classified Information	prohibited;2. Connection of unclassified mobile devices to unclassified systems requires approval from the authorizing official;3. Use of internal or external modems or wireless interfaces within the unclassified	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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		AC-20
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-20(03)	Use of External Systems | Non-organizationally Owned Systems — Restricted Use	Restrict the use of non-organizationally owned systems or system components to process, store, or transmit organizational information using [Assignment: organization-defined restrictions].	Functional	Equal	Organizationally Owned Technology Assets, Applications and/or Services	DCH-13.4	Mechanisms exist to restrict the use of non-organizationally owned Technology Assets, Applications and/or Services	10		
AC-20(04)	Use of External Systems | Network Accessible Storage Devices — Prohibited Use	Prohibit the use of [Assignment: organization-defined network accessible storage devices] in external systems.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-20(05)	Use of External Systems | Portable Storage Devices — Prohibited Use	Prohibit the use of organization-controlled portable storage devices by authorized individuals on external systems.	Functional	Equal	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	10		
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-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	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5		
AC-21(01)	Information Sharing | Automated Decision Support	Employ [Assignment: organization-defined automated mechanisms] to enforce information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-21(02)	Information Sharing | Information Search and Retrieval	Implement information search and retrieval services that enforce [Assignment: organization-defined information sharing restrictions].	Functional	Equal	Information Search & Retrieval	DCH-14.1	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) implement data search and	10		
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		AC-22
AC-23	Data Mining Protection	Employ [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to detect and protect against unauthorized data mining.	Functional	Intersects With	Data Mining Protection	DCH-16	Mechanisms exist to protect data storage objects against unauthorized data mining and data harvesting techniques.	5		
AC-23	Data Mining Protection	Employ [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to detect and protect against unauthorized data mining.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data	5		
AC-24	Access Control Decisions	[Selection (one or more): Establish procedures; Implement mechanisms] to ensure [Assignment: organization-defined access control decisions] are applied to each access request prior to access	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		
AC-24(01)	Access Control Decisions | Transmit Access Authorization Information	transmit [Assignment: organization-defined access authorization information] using [Assignment: organization-defined controls] to [Assignment: organization-defined systems] that enforce access control decisions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-24(02)	Access Control Decisions | No User or Process Identity	Enforce access control decisions based on [Assignment: organization-defined security or privacy attributes] that do not include the identity of the user or process acting on behalf of the user.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AC-25	Reference Monitor	Implement a reference monitor for [Assignment: organization-defined access control policies] that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.	Functional	Equal	Reference Monitor	IAC-27	reference monitor that is tamperproof, always-invoked, small enough to be subject to analysis / testing and the completeness of which can be	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	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	NIST SP 800-82 Low Overlay
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	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10		
AT-01	Policy and Procedures	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-01
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
AT-02(01)	Literacy Training and Awareness | Practical Exercises	Provide practical exercises in literacy training that simulate events and incidents.	Functional	Intersects With	Simulated Cyber Attack Scenario Training	SAT-02.1	Mechanisms exist to include simulated actual cyber-attacks through practical exercises that are aligned with current threat scenarios.	5		
AT-02(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(02)
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-02(05)	Literacy Training and Awareness | Advanced Persistent Threat	Provide literacy training on the advanced persistent threat.	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-03.2	training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous	5		
AT-02(06)	Literacy Training and Awareness | Cyber Threat Environment	a. Provide literacy training on the cyber threat environment; andb. Reflect current cyber threat information in system operations.	Functional	Equal	Cyber Threat Environment	SAT-03.6	role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day	10		
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	(1) Before authorizing access to the system or performing assigned duties; (2) When required by system	5		AT-03
AT-03(01)	Role-based Training | Environmental Controls	Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of environmental controls.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AT-03(02)	Role-based Training | Physical Security Controls	Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of physical security controls.	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 required by system	5		
AT-03(03)	Role-based Training | Practical Exercises	Provide practical exercises in security and privacy training that reinforce training objectives.	Functional	Equal	Practical Exercises	SAT-03.1	Mechanisms exist to include practical exercises in security, compliance and resilience training that reinforce training objectives.	10		
AT-03(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
AT-03(05)	Role-based Training | Processing Personally Identifiable Information	Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of personally identifiable information processing and transparency controls.	Functional	Equal	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated	10		
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	(1) Initial security, compliance and resilience awareness training; (2) Recurring awareness training; and	10		AT-04
AT-05		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
AT-06	Training Feedback	Provide feedback on organizational training results to the following personnel [Assignment: organization-defined frequency]: [Assignment: organization-defined personnel].	Functional	Intersects With	Simulated Cyber Attack Scenario Training	SAT-02.1	Mechanisms exist to include simulated actual cyber-attacks through practical exercises that are aligned with current threat scenarios.	5		
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
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
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-01
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 selection criteria for events to be logged;c. Specify	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
AU-02	Event Logging	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-02
AU-02(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
AU-02(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
AU-02(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
AU-02(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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
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-03(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
AU-03(03)	Records | Limit Personally Identifiable Information	Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: [Assignment: organization-defined elements].	Functional	Equal	Limit Personal Data (PD) In Audit Records	MON-03.5	Mechanisms exist to limit Personal Data (PD) contained in audit records to the elements identified in the Data Privacy Risk	10		
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
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-04(01)
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
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		

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	NIST SP 800-82 Low Overlay
AU-05(03)	Response to Audit Logging Process Failures | Configurable Traffic Volume Thresholds	Enforce configurable network communications traffic volume thresholds reflecting limits on audit log storage capacity and [Selection: reject; delay] network traffic above those thresholds.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AU-05(04)	Response to Audit Logging Process Failures | Shutdown on Failure	system shutdown; degraded operational mode with limited mission or business functionality available] in the event of [Assignment: organization-defined audit logging failures], unless an alternate audit logging	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AU-05(05)	Response to Audit Logging Process Failures | Alternate Audit Logging Capability	Provide an alternate audit logging capability in the event of a failure in primary audit logging capability that implements [Assignment: organization-defined alternate audit logging functionality].	Functional	Equal	Alternate Event Logging Capability	MON-13	Mechanisms exist to provide an alternate event logging capability in the event of a failure in primary audit capability.	10		
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
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
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(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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(04)	Audit Record Review, Analysis, and Reporting | Central Review and Analysis	Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.	Functional	Equal	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	10		
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		
AU-06(07)	Audit Record Review, Analysis, and Reporting | Permitted Actions	Specify the permitted actions for each [Selection (one or more): system process; role; user] associated with the review, analysis, and reporting of audit record information.	Functional	Equal	Permitted Actions	MON-02.5	Mechanisms exist to specify the permitted actions for both users and Technology Assets, Applications and/or Services	10		
AU-06(08)	Review, Analysis, and Reporting | Full Text Analysis of Privileged	Perform a full text analysis of logged privileged commands in a physically distinct component or subsystem of the system, or other system that is dedicated to that analysis.	Functional	Equal	Privileged Functions Logging	MON-03.3	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	10		
AU-06(09)	Review, Analysis, and Reporting | Correlation with Information from Nontechnical	Correlate information from nontechnical sources with audit record information to enhance 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(10)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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-07(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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
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-08
AU-08(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
AU-08(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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
AU-09(01)	Protection of Audit Information | Hardware Write-once Media	Write audit trails to hardware-enforced, write-once media.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AU-09(02)	Protection of Audit Information | Store on Separate Physical Systems or Components	Store audit records [Assignment: organization-defined frequency] in a repository that is part of a physically different system or system component than the system or component being audited.	Functional	Intersects With	Event Log Backup on Separate Physical Systems / Components	MON-08.1	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-09(05)	Protection of Audit Information | Dual Authorization	Enforce dual authorization for [Selection (one or more): movement; deletion] of [Assignment: organization-defined audit information].	Functional	Equal	Dual Authorization for Event Log Movement	MON-08.4	Automated mechanisms exist to enforce dual authorization for the movement or deletion of event logs.	10		
AU-09(06)	Protection of Audit Information | Read-only Access	Authorize read-only access to audit information to [Assignment: organization-defined subset of privileged users or roles].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AU-09(07)	Protection of Audit Information | Store on Component with Different Operating System	Store audit information on a component running a different operating system than the system or component being audited.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AU-10	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-10(01)	Non-repudiation | Association of Identities	a. Bind the identity of the information producer with the information to [Assignment: organization-defined strength of binding]; andb. Provide the means for authorized individuals to determine the identity of the producer of the information.	Functional	Intersects With	Identity Binding	MON-09.1	Mechanisms exist to bind the identity of the information producer to the information generated.	5		
AU-10(02)	Non-repudiation | Validate Binding of Information Producer Identity	a. Validate the binding of the information producer identity to the information at [Assignment: organization-defined frequency]; andb. Perform [Assignment: organization-defined actions] in the event of a validation error.	Functional	Intersects With	Identity Binding	MON-09.1	Mechanisms exist to bind the identity of the information producer to the information generated.	5		
AU-10(03)	Non-repudiation | Chain of Custody	Maintain reviewer or releaser credentials within the established chain of custody for information reviewed or released.	Functional	Intersects With	Chain of Custody & Forensics	IRO-08	digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-	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	NIST SP 800-82 Low Overlay
AU-10(04)	Non-repudiation | Validate Binding of Information Reviewer Identity	identity to the information at the transfer or release points prior to release or transfer between [Assignment: organization-defined security domains]; andb. Perform [Assignment: organization-defined	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AU-10(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
AU-11	Audit Record Retention	Retain audit records in [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.	Functional	Equal	Event Log Retention	MON-10	with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and	10		AU-11
AU-11(01)	Audit Record Retention | Long-term Retrieval Capability	Employ [Assignment: organization-defined measures] to ensure that long-term audit records generated by the system can be retrieved.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AU-12	Audit Record Generation	defined in AU-2a on [Assignment: organization-defined 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
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(02)	Audit Record Generation | Standardized Formats	Produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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		
AU-12(04)	Generation | Query Parameter Audits of Personally Identifiable	Provide and implement the capability for auditing the parameters of user query events for data sets containing personally identifiable information.	Functional	Equal	Query Parameter Audits of Personal Data (PD)	MON-06.1	Mechanisms exist to provide and implement the capability for auditing the parameters of user query events for data sets containing Personal Data (PD)	10		
AU-13	Monitoring for Information Disclosure	[Assignment: organization-defined frequency] for evidence of unauthorized disclosure of organizational information; andb. If an information disclosure is discovered:1. Notify [Assignment: organization-defined personnel or roles]; and2. Take the following additional	Functional	Equal	Monitoring For Information Disclosure	MON-11	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of non-public information.	10		
AU-13(01)	Monitoring for Information Disclosure | Use of Automated Tools	Monitor open-source information and information sites using [Assignment: organization-defined automated mechanisms].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AU-13(02)	Monitoring for Information Disclosure | Review of Monitored Sites	Review the list of open-source information sites being monitored [Assignment: organization-defined frequency].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AU-13(03)	Information Disclosure | Unauthorized Replication of	Employ discovery techniques, processes, and tools to determine if external entities are replicating organizational information in an unauthorized manner.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AU-14	Session Audit	[Selection (one or more): record; view; hear; log] the content of a user session under [Assignment: organization-defined circumstances]; andb. Develop, integrate, and use session auditing activities in consultation with legal counsel and in accordance with	Functional	Equal	Session Audit	MON-12	can: (1) Capture and log all content related to a user session; and (2) Remotely view all content	10		
AU-14(01)	Session Audit | System Start-up	Initiate session audits automatically at system start-up.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
AU-14(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
AU-14(03)	Session Audit | Remote Viewing and Listening	Provide and implement the capability for authorized users to remotely view and hear content related to an established user session in real time.	Functional	Equal	Real-Time Session Monitoring	MON-01.17	to remotely view and hear content related to an established user session in real time, in accordance with organizational standards, as well as statutory	10		
AU-15		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
AU-16	Cross-organizational Audit Logging	Employ [Assignment: organization-defined methods] for coordinating [Assignment: organization-defined audit information] among external organizations when audit information is transmitted across organizational boundaries	Functional	Intersects With	Cross-Organizational Monitoring	MON-14	external organizations to identify anomalous events when event logs are shared across organizational boundaries,	5		
AU-16(01)	Cross-organizational Audit Logging | Identity Preservation	Preserve the identity of individuals in cross-organizational audit trails.	Functional	Intersects With	Cross-Organizational Monitoring	MON-14	external organizations to identify anomalous events when event logs are shared across organizational boundaries,	5		
AU-16(02)	Cross-organizational Audit Logging | Sharing of Audit Information	Provide cross-organizational audit information to [Assignment: organization-defined organizations] based on [Assignment: organization-defined cross-organizational sharing agreements].	Functional	Equal	Sharing of Event Logs	MON-14.1	Mechanisms exist to share event logs with third-party organizations based on specific cross-organizational sharing agreements	10		
AU-16(03)	Cross-organizational Audit Logging | Disassociability	Implement [Assignment: organization-defined measures] to disassociate individuals from audit information transmitted across organizational boundaries.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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
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
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-01
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
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
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
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
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
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-02(03)	Control Assessments | Leveraging Results from External Organizations	Leverage the results of control assessments performed by [Assignment: organization-defined external organization(s)] on [Assignment: organization-defined system] when the assessment meets [Assignment: organization-defined requirements]	Functional	Equal	Third-Party Assessment Reciprocity	IAO-02.3	Mechanisms exist to accept and respond to the results of external assessments that are performed by impartial, external organizations	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	NIST SP 800-82 Low Overlay
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
CA-03(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
CA-03(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
CA-03(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
CA-03(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
CA-03(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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-03(07)	Information Exchange | Transitive Information Exchanges	exchanges with other systems through the systems identified in CA-3a; andb. Take measures to ensure that transitive (downstream) information exchanges cease when the controls on identified transitive	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
CA-04		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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-05
CA-05(01)	Plan of Action and Milestones | Automation Support for Accuracy and Currency	Ensure the accuracy, currency, and availability of the plan of action and milestones for the system using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Deficiency Tracking Automation	IAO-05.1	help ensure tracked deficiencies are: (1) Accurate; (2) Up-to-date; and	10		
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-06
CA-06(01)	Authorization | Joint Authorization — Intra-organization	Employ a joint authorization process for the system that includes multiple authorizing officials from the same organization conducting the authorization.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
CA-06(02)	Authorization | Joint Authorization — Inter-organization	Employ a joint authorization process for the system that includes multiple authorizing officials with at least one authorizing official from an organization external to the organization conducting the authorization.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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
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		
CA-07(01)	Continuous Monitoring | Types of Assessments	Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	security, compliance and resilience controls oversight function that reports to the organization's executive	5		
CA-07(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
CA-07(03)	Continuous Monitoring | Trend Analyses	Employ trend analyses to determine if control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data	Functional	Equal	Trend Analysis Reporting	MON-06.2	security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process	10		
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-07(04)
CA-07(05)	Continuous Monitoring | Consistency Analysis	Employ the following actions to validate that policies are established and implemented controls are operating in a consistent manner: [Assignment: organization-defined actions].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
CA-07(06)	Continuous Monitoring | Automation Support for Monitoring	Ensure the accuracy, currency, and availability of monitoring results for the system using [Assignment: organization-defined automated mechanisms].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
CA-08	Penetration Testing	Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components].	Functional	Equal	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	10		
CA-08(01)	Penetration Testing | Independent Penetration Testing Agent or Team	Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.	Functional	Equal	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	10		
CA-08(02)	Penetration Testing | Red Team Exercises	Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement: [Assignment: organization-defined red team exercises]	Functional	Equal	Red Team Exercises	VPM-10	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise Technology Assets,	10		
CA-08(03)	Penetration Testing | Facility Penetration Testing	Employ a penetration testing process that includes [Assignment: organization-defined frequency] [Selection (one or more): announced; unannounced] attempts to bypass or circumvent controls associated with physical access points to the facility	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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		CA-09
CA-09(01)	Internal System Connections | Compliance Checks	Perform security and privacy compliance checks on constituent system components prior to the establishment of the internal connection.	Functional	Equal	Endpoint Security Validation	NET-14.7	Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions, patch levels,	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
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
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-01
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
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
CM-02(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
CM-02(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn

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	NIST SP 800-82 Low Overlay
CM-02(06)	Baseline Configuration | Development and Test Environments	Maintain a baseline configuration for system development and test environments that is managed separately from the operational baseline configuration.	Functional	Equal	Development & Test Environment Configurations	CFG-02.4	Mechanisms exist to manage baseline configurations for development and test environments separately from operational baseline configurations to minimize the	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;andg. 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)	Change Control | Automated Documentation, Notification, and Prohibition of	configuration-controlled changes to the system; andg. 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)	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(02)	Configuration Change Control | Testing, Validation, and Documentation of Changes	Test, validate, and document changes to the system before finalizing the implementation of the changes.	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	appropriately test and document proposed changes in a non-production environment before changes are implemented in a	5		
CM-03(03)	Configuration Change Control | Automated Change Implementation	Implement changes to the current system baseline and deploy the updated baseline across the installed base using [Assignment: organization-defined automated mechanisms].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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(05)	Configuration Change Control | Automated Security Response	Implement the following security responses automatically if baseline configurations are changed in an unauthorized manner: [Assignment: organization-defined security responses].	Functional	Equal	Automated Security Response	CHG-02.4	Automated mechanisms exist to implement remediation actions upon the detection of unauthorized baseline configurations change(s).	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-03(07)	Configuration Change Control | Review System Changes	Review changes to the system [Assignment: organization-defined frequency] or when [Assignment: organization-defined circumstances] to determine whether unauthorized changes have occurred.	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	appropriately test and document proposed changes in a non-production environment before changes are implemented in a	5		
CM-03(08)	Configuration Change Control | Prevent or Restrict Configuration Changes	Prevent or restrict changes to the configuration of the system under the following circumstances: [Assignment: organization-defined circumstances].	Functional	Equal	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.	10		
CM-03(08)	Configuration Change Control | Prevent or Restrict Configuration Changes	Prevent or restrict changes to the configuration of the system under the following circumstances: [Assignment: organization-defined circumstances].	Functional	Intersects With	Integrity Assurance & Enforcement (IAE)	CFG-06.1	identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the	5		
CM-04	Impact Analyses	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.	Functional	Equal	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	10		CM-04
CM-04(01)	Impact Analyses | Separate Test Environments	Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.	Functional	Equal	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized	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 (IA) 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
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
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-05(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
CM-05(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
CM-05(04)	Access Restrictions for Change | Dual Authorization	Enforce dual authorization for implementing changes to [Assignment: organization-defined system components and system-level information].	Functional	Equal	Dual Authorization for Change	CHG-04.3	Mechanisms exist to enforce a two-person rule for implementing changes to critical Technology Assets, Applications and/or	10		
CM-05(05)	Access Restrictions for Change | Privilege Limitation for Production and Operation	a. Limit privileges to change system components and system-related information within a production or operational environment; andb. Review and reevaluate privileges [Assignment: organization-defined frequency].	Functional	Equal	Permissions To Implement Changes	CHG-04.4	Mechanisms exist to limit operational privileges for implementing changes.	10		
CM-05(06)	Access Restrictions for Change | Limit Library Privileges	Limit privileges to change software resident within software libraries.	Functional	Equal	Library Privileges	CHG-04.5	Mechanisms exist to restrict software library privileges to those individuals with a pertinent business need for access.	10		
CM-05(07)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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
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
CM-06(01)	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-06(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
CM-06(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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	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
CM-07(01)	Least Functionality | Periodic Review	restricted functions, system ports, protocols, software, 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	NIST SP 800-82 Low Overlay
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	Functional	Intersects With	Prevent Program Execution	SEA-06	Automated mechanisms exist to prevent the execution of unauthorized software programs.	5		
CM-07(02)	Least Functionality | Prevent Program Execution	[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	Functional	Intersects With	Prevent Unauthorized Software Execution	CFG-03.2	Mechanisms exist to configure systems to prevent the execution of unauthorized software programs.	5		
CM-07(03)	Least Functionality | Registration Compliance	Ensure compliance with [Assignment: organization-defined registration requirements for functions, ports, protocols, and services].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
CM-07(04)	Least Functionality | Unauthorized Software — Deny-by-exception	programs not authorized to execute on the system];b. Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; andc. Review and update the list of unauthorized software programs [Assignment:	Functional	Equal	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	10		
CM-07(05)	Least Functionality | Authorized Software — Allow-by-exception	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	Equal	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	10		
CM-07(06)	Least Functionality | Confined Environments with Limited Privileges	Require that the following user-installed software execute in a confined physical or virtual machine environment with limited privileges: [Assignment: organization-defined user-installed software].	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more	5		
CM-07(07)	Least Functionality | Code Execution in Protected Environments	only in confined physical or virtual machine environments and with the explicit approval of [Assignment: organization-defined personnel or roles] when such code is:a. Obtained from sources with	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more	5		
CM-07(08)	Least Functionality | Binary or Machine Executable Code	code from sources with limited or no warranty or without the provision of source code; andb. Allow exceptions only for compelling mission or operational requirements and with the approval of the authorizing	Functional	Equal	Binary or Machine-Executable Code	END-06.7	Mechanisms exist to prohibit the use of binary or machine-executable code from sources with limited or no warranty and without access to source code.	10		
CM-07(09)	Least Functionality | Prohibiting The Use of Unauthorized Hardware	components authorized for system use];b. Prohibit the use or connection of unauthorized hardware components;c. Review and update the list of authorized hardware components [Assignment:	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more	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:	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
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
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	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-08(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
CM-08(06)	Inventory | Assessed Configurations and Approved	Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.	Functional	Equal	Approved Baseline Deviations	AST-02.4	Mechanisms exist to document and govern instances of approved deviations from established baseline configurations.	10		
CM-08(07)	System Component Inventory | Centralized Repository	Provide a centralized repository for the inventory of system components.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-	5		
CM-08(08)	System Component Inventory | Automated Location Tracking	Support the tracking of system components by geographic location using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Automated Location Tracking	AST-02.10	Mechanisms exist to track the geographic location of system components.	10		
CM-08(09)	System Component Inventory | Assignment of Components to Systems	a. Assign system components to a system; andb. Receive an acknowledgement from [Assignment: organization-defined personnel or roles] of this assignment.	Functional	Equal	Component Assignment	AST-02.11	Mechanisms exist to bind components to a specific system.	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-09(01)	Configuration Management Plan | Assignment of Responsibility	Assign responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.	Functional	Equal	Assignment of Responsibility	CFG-01.1	Segregation of duties for configuration management that prevents developers from performing production configuration management.	10		
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-10
CM-10(01)	Software Usage Restrictions | Open-source Software	Establish the following restrictions on the use of open-source software: [Assignment: organization-defined restrictions].	Functional	Equal	Open Source Software	CFG-04.1	Mechanisms exist to establish parameters for the secure use of open source software.	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	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	5		
CM-11	User-installed Software	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-11
CM-11(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
CM-11(02)	User-installed Software | Software Installation with Privileged Status	Allow user installation of software only with explicit privileged status.	Functional	Intersects With	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5		
CM-11(02)	User-installed Software | Software Installation with Privileged Status	Allow user installation of software only with explicit privileged status.	Functional	Intersects With	Restrict Roles Permitted To Install Software	CFG-05.2	Mechanisms exist to configure systems to prevent the installation of software, unless the action is performed by a privileged user or service.	5		

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	NIST SP 800-82 Low Overlay
CM-11(02)	User-installed Software | Software Installation with Privileged Status	Allow user installation of software only with explicit privileged status.	Functional	Intersects With	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	5		
CM-11(03)	User-installed Software | Automated Enforcement and Monitoring	Enforce and monitor compliance with software installation policies using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.	5		
CM-11(03)	User-installed Software | Automated Enforcement and Monitoring	Enforce and monitor compliance with software installation policies using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Integrity Assurance & Enforcement (IAE)	CFG-06.1	identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the	5		
CM-11(03)	User-installed Software | Automated Enforcement and Monitoring	Enforce and monitor compliance with software installation policies using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Software Installation Alerts	END-03.1	Mechanisms exist to generate an alert when new software is detected.	5		
CM-11(03)	User-installed Software | Automated Enforcement and Monitoring	Enforce and monitor compliance with software installation policies using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Unauthorized Installation Alerts	CFG-05.1	Mechanisms exist to configure systems to generate an alert when the unauthorized installation of software is detected.	5		
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		
CM-13	Data Action Mapping	Develop and document a map of system data actions.	Functional	Equal	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where	10		
CM-14	Signed Components	Prevent the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.	Functional	Intersects With	Signed Components	CHG-04.2	installation of software and firmware components without verification that the component has been digitally signed using an organization-approved	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	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
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
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-01
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
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
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(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
CP-02(05)	Contingency Plan | Continue Mission and Business Functions	Plan for the continuance of [Selection (one): all; essential] mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.	Functional	Equal	Continue Essential Mission & Business Functions	BCD-02.2	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(06)	Contingency Plan | Alternate Processing and Storage Sites	mission and business functions to alternate processing and/or storage sites with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing	Functional	Equal	Transfer to Alternate Processing / Storage Site	BCD-01.3	Mechanisms exist to redeploy personnel to other roles during a disruptive event or in the execution of a continuity plan.	10		
CP-02(07)	Contingency Plan | Coordinate with External Service Providers	Coordinate the contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.	Functional	Equal	Coordinate With External Service Providers	BCD-01.2	internal contingency plans with the contingency plans of external service providers to ensure that contingency requirements can be	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
CP-03(01)	Contingency Training | Simulated Events	Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.	Functional	Equal	Simulated Events	BCD-03.1	Mechanisms exist to incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.	10		
CP-03(02)	Contingency Training | Mechanisms Used in Training Environments	Employ mechanisms used in operations to provide a more thorough and realistic contingency training environment.	Functional	Equal	Automated Training Environments	BCD-03.2	Automated mechanisms exist to provide a more thorough and realistic contingency training environment.	10		
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; and c. 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
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; and c. 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
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-04(03)	Contingency Plan Testing | Automated Testing	Test the contingency plan using [Assignment: organization-defined automated mechanisms].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-82 Low Overlay
CP-04(04)	Contingency Plan Testing | Full Recovery and Reconstitution	Include a full recovery and reconstitution of the system to a known state as part of contingency plan testing.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
CP-04(05)	Contingency Plan Testing | Self-challenge	Employ [Assignment: organization-defined mechanisms] to [Assignment: organization-defined system or system component] to disrupt and adversely affect the system or system component.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
CP-05		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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 disaster.	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	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	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-07(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
CP-07(06)	Alternate Processing Site | Inability to Return to Primary Site	Plan and prepare for circumstances that preclude returning to the primary processing site.	Functional	Equal	Inability to Return to Primary Site	BCD-09.5	Mechanisms exist to plan and prepare for both natural and manmade circumstances that preclude returning to the primary site.	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-08(05)	Telecommunications Services | Alternate Telecommunication Service Testing	Test alternate telecommunication services [Assignment: organization-defined frequency].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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
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	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(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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	backup data to the alternate storage site at a rate that is capable of meeting both Recovery Time Objectives (RTOs) and Recovery Point Objectives	10		
CP-09(06)	System Backup | Redundant Secondary System	Conduct system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations.	Functional	Equal	Redundant Secondary System	BCD-11.7	Mechanisms exist to maintain a failover capability, which is not collocated with the primary Technology Asset, Application	10		
CP-09(07)	System Backup | Dual Authorization for Deletion or Destruction	Enforce dual authorization for the deletion or destruction of [Assignment: organization-defined backup information].	Functional	Equal	Dual Authorization For Backup Media Destruction	BCD-11.8	Mechanisms exist to implement and enforce dual authorization for the deletion or destruction of sensitive backup media and data.	10		
CP-09(08)	System Backup | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined backup information].	Functional	Equal	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	10		
CP-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	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
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
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
CP-10(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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		

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	NIST SP 800-82 Low Overlay
CP-10(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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		
CP-10(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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-11	Alternate Communications Protocols	Provide the capability to employ [Assignment: organization-defined alternative communications protocols] in support of maintaining continuity of operations.	Functional	Intersects With	Telecommunications Services Availability	BCD-10	Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services.	5		
CP-12	Safe Mode	When [Assignment: organization-defined conditions] are detected, enter a safe mode of operation with [Assignment: organization-defined restrictions of safe mode of operation].	Functional	Intersects With	Fail Secure	SEA-07.2	systems to fail to an organization-defined known-state for types of failures, preserving system state information in	5		CP-12
CP-13	Alternative Security Mechanisms	Employ [Assignment: organization-defined alternative or supplemental security mechanisms] for satisfying [Assignment: organization-defined security functions] when the primary means of implementing the security function is unavailable or compromised.	Functional	Equal	Alternative Security Measures	BCD-07	alternative or compensating controls to satisfy security functions when the primary means of implementing the security function is unavailable	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	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
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
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-01
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
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)
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)
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)
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)
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)
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)
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(01)
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)
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)
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)
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)
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)
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)
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(02)
IA-02(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
IA-02(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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(06)	Authentication (organizational Users) | Access to Accounts —	[Selection (one or more): privileged accounts; non-privileged accounts] such that:a. One of the factors is provided by a device separate from the system gaining access; andb. The device meets [Assignment:	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(07)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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(08)
IA-02(09)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
IA-02(10)	Identification and Authentication (organizational Users) | Single Sign-on	Provide a single sign-on capability for [Assignment: organization-defined system accounts and services].	Functional	Equal	Single Sign-On (SSO) Transparent Authentication	IAC-13.1	Mechanisms exist to provide a transparent authentication (e.g., Single Sign-On (SSO)) capability to the organization's Technology	10		
IA-02(11)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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-02(12)
IA-02(13)	Identification and Authentication (organizational Users) | Out-of-band Authentication	Implement the following out-of-band authentication mechanisms under [Assignment: organization-defined conditions]: [Assignment: organization-defined out-of-band authentication].	Functional	Equal	Out-of-Band Authentication (OOBA)	IAC-02.4	Mechanisms exist to implement Out-of-Band Authentication (OOBA) under specific conditions.	10		

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	NIST SP 800-82 Low Overlay
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-03
IA-03(01)	Identification and Authentication | Cryptographic Bidirectional	Authenticate [Assignment: organization-defined devices and/or types of devices] before establishing [Selection (one or more): local; remote; network] connection using bidirectional authentication that is cryptographically based.	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that	5		
IA-03(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
IA-03(03)	Device Identification and Authentication | Dynamic Address Allocation	standardize dynamic address allocation lease information and the lease duration assigned to devices in accordance with [Assignment: organization-defined lease information and lease duration]; andb. Audit	Functional	Intersects With	Network Access Control (NAC)	AST-02.5	employ Network Access Control (NAC), or a similar technology, which is capable of detecting unauthorized devices and disable network access to those	5		
IA-03(04)	Device Identification and Authentication | Device Attestation	Handle device identification and authentication based on attestation by [Assignment: organization-defined configuration management process].	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that	5		
IA-03(04)	Device Identification and Authentication | Device Attestation	Handle device identification and authentication based on attestation by [Assignment: organization-defined configuration management process].	Functional	Intersects With	Device Attestation	IAC-04.1	Device identification and authentication is accurate by centrally-managing the joining of systems to the domain as part of the initial asset configuration	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
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
IA-04(01)	Identifier Management | Prohibit Account Identifiers as Public Identifiers	Prohibit the use of system account identifiers that are the same as public identifiers for individual accounts.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
IA-04(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
IA-04(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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		
IA-04(05)	Identifier Management | Dynamic Management	Manage individual identifiers dynamically in accordance with [Assignment: organization-defined dynamic identifier policy].	Functional	Intersects With	Dynamic Management	IAC-09.3	Mechanisms exist to dynamically manage usernames and system identifiers.	5		
IA-04(06)	Identifier Management | Cross-organization Management	Coordinate with the following external organizations for cross-organization management of identifiers: [Assignment: organization-defined external organizations].	Functional	Equal	Cross-Organization Management	IAC-09.4	Mechanisms exist to coordinate username identifiers with external organizations for cross-organization management of identifiers	10		
IA-04(07)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
IA-04(08)	Identifier Management | Pairwise Pseudonymous Identifiers	Generate pairwise pseudonymous identifiers.	Functional	Equal	Pairwise Pseudonymous Identifiers (PPID)	IAC-09.6	pairwise pseudonymous identifiers with no identifying information about a data subject to discourage activity tracking	10		
IA-04(09)	Identifier Management | Attribute Maintenance and Protection	Maintain the attributes for each uniquely identified individual, device, or service in [Assignment: organization-defined protected central storage].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and	5		IA-05
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
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	determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity	5		IA-05(01)
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)
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(01)
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	validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for	10		
IA-05(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
IA-05(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
IA-05(05)	Authenticator Management | Change Authenticators Prior to Delivery	Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.	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(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	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-05(07)	Authenticator Management | No Embedded Unencrypted Static Authenticators	Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.	Functional	Equal	No Embedded Unencrypted Static Authenticators	IAC-10.6	Mechanisms exist to ensure that unencrypted, static authenticators are not embedded in applications, scripts or stored on function keys	10		
IA-05(08)	Authenticator Management | Multiple System Accounts	Implement [Assignment: organization-defined security controls] to manage the risk of compromise due to individuals having accounts on multiple systems.	Functional	Intersects With	Multiple System Accounts	IAC-10.9	Mechanisms exist to implement security safeguards to manage the risk of compromise due to individuals having accounts on	5		
IA-05(08)	Authenticator Management | Multiple System Accounts	Implement [Assignment: organization-defined security controls] to manage the risk of compromise due to individuals having accounts on multiple systems.	Functional	Intersects With	Privileged Account Identifiers	IAC-09.5	Mechanisms exist to uniquely manage privileged accounts to identify the account as a privileged user or service.	5		
IA-05(09)	Authenticator Management | Federated Credential Management	Use the following external organizations to federate credentials: [Assignment: organization-defined external organizations].	Functional	Equal	Federated Credential Management	IAC-13.2	Mechanisms exist to federate credentials to allow cross-organization authentication of individuals and devices.	10		
IA-05(10)	Authenticator Management | Dynamic Credential Binding	Bind identities and authenticators dynamically using the following rules: [Assignment: organization-defined binding rules].	Functional	Intersects With	Dynamic Management	IAC-09.3	Mechanisms exist to dynamically manage usernames and system identifiers.	5		
IA-05(11)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn

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	NIST SP 800-82 Low Overlay
IA-05(12)	Authenticator Management | Biometric Authentication Performance	For biometric-based authentication, employ mechanisms that satisfy the following biometric quality requirements [Assignment: organization-defined biometric quality requirements].	Functional	Equal	Biometric Authentication	IAC-10.12	biometric-based authentication satisfies organization-defined biometric quality requirements for false positives and false	10		
IA-05(13)	Authenticator Management | Expiration of Cached Authenticators	Prohibit the use of cached authenticators after [Assignment: organization-defined time period].	Functional	Equal	Expiration of Cached Authenticators	IAC-10.10	Automated mechanisms exist to prohibit the use of cached authenticators after organization-defined time period.	10		
IA-05(14)	Authenticator Management | Managing Content of PKI Trust Stores	For PKI-based authentication, employ an organization-wide methodology for managing the content of PKI trust stores installed across all platforms, including networks, operating systems, browsers, and applications.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
IA-05(15)	Authenticator Management | GSA-approved Products and Services	Use only General Services Administration-approved products and services for identity, credential, and access management.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
IA-05(16)	Management | In-person or Trusted External Party Authenticator	organization-defined types of and/or specific authenticators] be conducted [Selection (one): in person; by a trusted external party] before [Assignment: organization-defined registration authority] with authorization by [Assignment:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
IA-05(17)	Management | Presentation Attack Detection for Biometric	Employ presentation attack detection mechanisms for biometric-based authentication.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
IA-05(18)	Authenticator Management | Password Managers	a. Employ [Assignment: organization-defined password managers] to generate and manage passwords; andb. Protect the passwords using [Assignment: organization-defined controls].	Functional	Equal	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	10		
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	feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized	10		IA-06
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
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-07
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
IA-08(01)	Identification and Authentication (non-organizational Users) | Acceptance of PIV Credentials from Other Organizations	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(01)
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(02)
IA-08(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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-08(04)
IA-08(05)	Identification and Authentication (non-organizational Users) | Acceptance of PIV Credentials	Accept and verify federated or PKI credentials that meet [Assignment: organization-defined policy].	Functional	Equal	Acceptance of PIV Credentials	IAC-02.3	Mechanisms exist to accept and electronically verify organizational Personal Identity Verification (PIV) credentials.	10		
IA-08(06)	Authentication (non-organizational Users) | Disassociability	Implement the following measures to disassociate user attributes or identifier assertion relationships among individuals, credential service providers, and relying parties: [Assignment: organization-defined measures].	Functional	Equal	Disassociability	IAC-03.4	Mechanisms exist to disassociate user attributes or credential assertion relationships among individuals, credential service providers and relying parties	10		
IA-09	Service Identification and Authentication	Uniquely identify and authenticate [Assignment: organization-defined system services and applications] before establishing communications with devices, users, or other services or applications.	Functional	Equal	Authentication for Third-Party Technology Assets, Applications and/or	IAC-05	Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).	10		
IA-09(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
IA-09(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
IA-10	Adaptive Authentication	Require individuals accessing the system to employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific [Assignment: organization-defined circumstances or situations].	Functional	Equal	Adaptive Identification & Authentication	IAC-13	Mechanisms exist to allow individuals to utilize alternative methods of authentication under specific circumstances or situations	10		
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-11
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		
IA-12(06)	Identity Proofing | Accept Externally-proofed Identities	Accept externally-proofed identities at [Assignment: organization-defined identity assurance level].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
IA-13	Identity Providers and Authorization Servers	manage user, device, and non-person entity (NPE) identities, attributes, and access rights supporting authentication and authorization decisions in accordance with [Assignment: organization-defined identification and authentication policy] using	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
IA-13(01)	Protection of Cryptographic Keys	Cryptographic keys that protect access tokens are generated, managed, and protected from disclosure and misuse.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-82 Low Overlay
IA-13(02)	Verification of Identity and Access Tokens	The source and integrity of identity assertions and access tokens are verified before granting access to system and information resources.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
IA-13(03)	Token Management	In accordance with [Assignment: organization-defined identification and authentication policy], assertions and access tokens are:a. generated;b. issued; c. refreshed;d. revoked;e. time-restricted; andf. audience-restricted.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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
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
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
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
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		IR-01
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
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-02(03)	Incident Response Training | Breach	Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5		
IR-03	Incident Response Testing	Test the effectiveness of the incident response capability for the system [Assignment: organization-defined frequency] using the following tests: [Assignment: organization-defined tests].	Functional	Intersects With	Incident Response Testing	IRO-06	incident response capabilities through realistic exercises to determine the operational effectiveness of those	5		
IR-03(01)	Incident Response Testing | Automated Testing	Test the incident response capability using [Assignment: organization-defined automated mechanisms].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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-03(03)	Incident Response Testing | Continuous Improvement	Determine the effectiveness of incident response processes;b. Continuously improve incident response processes; andc. Provide incident response measures and metrics that are accurate, consistent, and in a	Functional	Equal	Continuous Incident Response Improvements	IRO-04.3	(1) Determine the effectiveness of incident response processes; (2) Continuously improve incident response processes; and	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
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(02)	Incident Handling | Dynamic Reconfiguration	Include the following types of dynamic reconfiguration for [Assignment: organization-defined system components] as part of the incident response capability: [Assignment: organization-defined types of dynamic reconfiguration]	Functional	Equal	Dynamic Reconfiguration	IRO-02.3	Automated mechanisms exist to dynamically reconfigure system components as part of the incident response capability.	10		
IR-04(03)	Incident Handling | Continuity of Operations	incidents] and take the following actions in response to those incidents to ensure continuation of organizational mission and business functions: [Assignment: organization-defined actions to take in	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		
IR-04(03)	Incident Handling | Continuity of Operations	incidents] and take the following actions in response to those incidents to ensure continuation of organizational mission and business functions: [Assignment: organization-defined actions to take in	Functional	Intersects With	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	5		
IR-04(04)	Incident Handling | Information Correlation	Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	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(05)	Incident Handling | Automatic Disabling of System	Implement a configurable capability to automatically disable the system if [Assignment: organization-defined security violations] are detected.	Functional	Intersects With	Automated Response to Suspicious Events	MON-01.11	Automated mechanisms exist to implement pre-determined corrective actions in response to detected events that have	5		
IR-04(05)	Incident Handling | Automatic Disabling of System	Implement a configurable capability to automatically disable the system if [Assignment: organization-defined security violations] are detected.	Functional	Intersects With	Automatic Disabling of Technology Assets, Applications and/or Services (TAAS)	IRO-02.6	Mechanisms exist to automatically disable Technology Assets, Applications and/or Services (TAAS), upon detection	5		
IR-04(06)	Incident Handling | Insider Threats	Implement an incident handling capability for incidents involving insider threats.	Functional	Intersects With	Insider Threat Response Capability	IRO-02.2	Mechanisms exist to implement and govern an insider threat program.	5		
IR-04(07)	Incident Handling | Insider Threats — Intra-organization Coordination	Coordinate an incident handling capability for insider threats that includes the following organizational entities [Assignment: organization-defined entities].	Functional	Intersects With	Insider Threat Response Capability	IRO-02.2	Mechanisms exist to implement and govern an insider threat program.	5		
IR-04(08)	Incident Handling | Correlation with External Organizations	external organizations] to correlate and share [Assignment: organization-defined incident information] to achieve a cross-organization perspective on incident awareness and more effective	Functional	Equal	Correlation with External Organizations	IRO-02.5	with approved third-parties to achieve a cross-organization perspective on incident awareness and more effective	10		
IR-04(09)	Incident Handling | Dynamic Response Capability	Employ [Assignment: organization-defined dynamic response capabilities] to respond to incidents.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
IR-04(10)	Incident Handling | Supply Chain Coordination	Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5		
IR-04(10)	Incident Handling | Supply Chain Coordination	Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.	Functional	Intersects With	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity and data protection incident information to the provider of the Technology	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		

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	NIST SP 800-82 Low Overlay
IR-04(12)	Incident Handling | Malicious Code and Forensic Analysis	Analyze malicious code and/or other residual artifacts remaining in the system after the incident.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of	5		
IR-04(12)	Incident Handling | Malicious Code and Forensic Analysis	Analyze malicious code and/or other residual artifacts remaining in the system after the incident.	Functional	Intersects With	Chain of Custody & Forensics	IRO-08	digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-	5		
IR-04(13)	Incident Handling | Behavior Analysis	Analyze anomalous or suspected adversarial behavior in or related to [Assignment: organization-defined environments or resources].	Functional	Intersects With	Honeypots	SEA-11	honeypots that are specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting and	5		
IR-04(13)	Incident Handling | Behavior Analysis	Analyze anomalous or suspected adversarial behavior in or related to [Assignment: organization-defined environments or resources].	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to	5		
IR-04(13)	Incident Handling | Behavior Analysis	Analyze anomalous or suspected adversarial behavior in or related to [Assignment: organization-defined environments or resources].	Functional	Intersects With	Honeyclients	SEA-12	Mechanisms exist to utilize honeyclients that proactively seek to identify malicious websites and/or web-based malicious code.	5		
IR-04(14)	Incident Handling | Security Operations Center	Establish and maintain a security operations center.	Functional	Equal	Security Operations Center (SOC)	OPS-04	Mechanisms exist to establish and maintain a Security Operations Center (SOC) that facilitates a 24x7 response capability.	10		
IR-04(15)	Incident Handling | Public Relations and Reputation Repair	a. Manage public relations associated with an incident; andb. Employ measures to repair the reputation of the organization.	Functional	Equal	Public Relations & Reputation Repair	IRO-16	associated with incidents and employ appropriate measures to prevent further reputational damage and develop plans to	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
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
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
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
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(02)	Incident Reporting | Vulnerabilities Related to Incidents	Report system vulnerabilities associated with reported incidents to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of	5		
IR-06(02)	Incident Reporting | Vulnerabilities Related to Incidents	Report system vulnerabilities associated with reported incidents to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Vulnerabilities Related To Incidents	IRO-10.3	system vulnerabilities associated with reported cybersecurity and data protection incidents to organization-defined personnel	5		
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
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-07(02)	Incident Response Assistance | Coordination with External Providers	a. Establish a direct, cooperative relationship between its incident response capability and external providers of system protection capability; andb. Identify organizational incident response team members to the external providers.	Functional	Equal	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	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		IR-08
IR-08(01)	Incident Response Plan | Breaches	information; A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;b. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals	Functional	Equal	Data Breach	IRO-04.1	data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and	10		
IR-09	Information Spillage Response	organization-defined personnel or roles] on the information spill using a method of communication not associated with the spill;d. Isolating the contaminated system or system component;e. Eradicating the	Functional	Intersects With	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive/regulated data spills.	5		
IR-09	Information Spillage Response	information from the contaminated system or information spill using a method of communication not associated with the spill;d. Isolating the contaminated system or system component;e. Eradicating the	Functional	Intersects With	Sensitive / Regulated Data Spill Responsible Personnel	IRO-12.1	Mechanisms exist to formally assign personnel or roles with responsibility for responding to sensitive/regulated data spills.	5		
IR-09(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
IR-09(02)	Information Spillage Response | Training	Provide information spillage response training [Assignment: organization-defined frequency].	Functional	Equal	Sensitive / Regulated Data Spill Training	IRO-12.2	Mechanisms exist to ensure incident response training material provides coverage for sensitive/regulated data spillage	10		
IR-09(03)	Information Spillage Response | Post-spill Operations	organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions: [Assignment: organization-defined	Functional	Equal	Post-Sensitive / Regulated Data Spill Operations	IRO-12.3	Mechanisms exist to ensure that organizational personnel impacted by sensitive/regulated data spills can continue to carry	10		
IR-09(04)	Information Spillage Response | Exposure to Unauthorized Personnel	Employ the following controls for personnel exposed to information not within assigned access authorizations: [Assignment: organization-defined controls].	Functional	Equal	Sensitive / Regulated Data Exposure to Unauthorized Personnel	IRO-12.4	Mechanisms exist to address security safeguards for personnel exposed to sensitive/regulated data that is not within their	10		
IR-10		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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 control across the enterprise	10		MA-01
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
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	Mechanisms exist to review the remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote	5		MA-01
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

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	NIST SP 800-82 Low Overlay
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-01
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
MA-02(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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		
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-03(04)	Maintenance Tools | Restricted Tool Use	Restrict the use of maintenance tools to authorized personnel only.	Functional	Equal	Restrict Tool Usage	MNT-04.4	Automated mechanisms exist to restrict the use of maintenance tools to authorized maintenance personnel and/or roles.	10		
MA-03(05)	Maintenance Tools | Execution with Privilege	Monitor the use of maintenance tools that execute with increased privilege.	Functional	Intersects With	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	5		
MA-03(06)	Maintenance Tools | Software Updates and Patches	Inspect maintenance tools to ensure the latest software updates and patches are installed.	Functional	Intersects With	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	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	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	5		MA-04
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
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
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(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
MA-04(03)	Nonlocal Maintenance | Comparable Security and Sanitization	implemented on the system being serviced; orb. Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational information); and after the service is performed,	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-04(04)	Nonlocal Maintenance | Authentication and Separation of Maintenance Sessions	employing [Assignment: organization-defined authenticators that are replay resistant]; andb. Separating the maintenance sessions from other network sessions with the system by either:1. Physically separated communications paths; or2.	Functional	Equal	Separation of Maintenance Sessions	MNT-05.7	maintenance sessions through replay-resistant sessions that are physically or logically separated communications paths from	10		
MA-04(05)	Nonlocal Maintenance | Approvals and Notifications	session by [Assignment: organization-defined personnel or roles]; andb. Notify the following personnel or roles of the date and time of planned nonlocal maintenance: [Assignment: organization-	Functional	Equal	Remote Maintenance Pre-Approval	MNT-05.5	Mechanisms exist to require maintenance personnel to obtain pre-approval and scheduling for remote, non-local maintenance sessions	10		
MA-04(06)	Nonlocal Maintenance | Cryptographic Protection	implement the following cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications: [Assignment: organization-defined cryptographic mechanisms]	Functional	Equal	Remote Maintenance Cryptographic Protection	MNT-05.3	Cryptographic mechanisms exist to protect the integrity and confidentiality of remote, non-local maintenance and diagnostic communications.	10		
MA-04(07)	Nonlocal Maintenance | Disconnect Verification	Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.	Functional	Equal	Remote Maintenance Disconnect Verification	MNT-05.4	Mechanisms exist to provide remote disconnect verification to ensure remote, non-local maintenance and diagnostic sessions are properly terminated	10		
MA-05	Maintenance Personnel	maintenance organizations or personnel;b. Verify that 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
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-05(02)	Maintenance Personnel | Security Clearances for Classified Systems	diagnostic activities on a system processing, storing, or transmitting classified information possess security clearances and formal access approvals for at least the highest classification level and for compartments of	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-05(03)	Maintenance Personnel | Citizenship Requirements for Classified Systems	Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information are U.S. citizens.	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-05(04)	Maintenance Personnel | Foreign Nationals	when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; andb. Approvals, consents, and detailed operational conditions regarding the use of foreign	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-05(05)	Maintenance Personnel | Non-system Maintenance	Ensure that non-escorted personnel performing maintenance activities not directly associated with the system but in the physical proximity of the system, have required access authorizations.	Functional	Equal	Non-System Related Maintenance	MNT-06.2	Mechanisms exist to ensure that non-escorted personnel performing non-IT maintenance activities in the physical	10		
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-06(01)	Timely Maintenance | Preventive Maintenance	Perform preventive maintenance on [Assignment: organization-defined system components] at [Assignment: organization-defined time intervals].	Functional	Equal	Preventative Maintenance	MNT-03.1	Mechanisms exist to perform preventive maintenance on critical Technology Assets, Applications and/or Services	10		
MA-06(02)	Timely Maintenance | Predictive Maintenance	Perform predictive maintenance on [Assignment: organization-defined system components] at [Assignment: organization-defined time intervals].	Functional	Equal	Predictive Maintenance	MNT-03.2	Mechanisms exist to perform predictive maintenance on critical Technology Assets, Applications and/or Services	10		
MA-06(03)	Timely Maintenance | Automated Support for Predictive Maintenance	Transfer predictive maintenance data to a maintenance management system using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Automated Support For Predictive Maintenance	MNT-03.3	Automated mechanisms exist to transfer predictive maintenance data to a computerized maintenance management system	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		MA-07

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	NIST SP 800-82 Low Overlay
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
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
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-01
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
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-02
MP-02(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
MP-02(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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 sanitized using approved equipment, techniques, and	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 destroyed or	10		
MP-04(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
MP-04(02)	Media Storage | Automated Restricted Access	Restrict access to media storage areas and log access attempts and access granted using [Assignment: organization-defined automated mechanisms].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
MP-05	Media Transport	outside of controlled areas using [Assignment: organization-defined controls];b. Maintain accountability for system media during transport outside of controlled areas;c. Document activities associated with the transport of system media; andd.	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-05(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
MP-05(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
MP-05(03)	Media Transport | Custodians	Employ an identified custodian during transport of system media outside of controlled areas.	Functional	Equal	Custodians	DCH-07.1	Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.	10		
MP-05(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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
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
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
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-06(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
MP-06(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
MP-06(06)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
MP-06(07)	Media Sanitization | Dual Authorization	Enforce dual authorization for the sanitization of [Assignment: organization-defined system media].	Functional	Equal	Dual Authorization for Sensitive Data Destruction	DCH-09.5	Mechanisms exist to enforce dual authorization for the destruction, disposal or sanitization of digital media that contains sensitive/regulated data	10		
MP-06(08)	Media Sanitization | Remote Purging or Wiping of Information	Provide the capability to purge or wipe information from [Assignment: organization-defined systems or system components] [Selection (one): remotely; under the following conditions: [Assignment: organization-defined conditions]]	Functional	Equal	Remote Purging	MDM-05	Mechanisms exist to remotely purge selected information from mobile devices.	10		
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		MP-07
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
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		MP-07
MP-07(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
MP-07(02)	Media Use | Prohibit Use of Sanitization-resistant Media	Prohibit the use of sanitization-resistant media in organizational systems.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
MP-08	Media Downgrading	classification of the information;b. Verify that the system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the	Functional	Intersects With	Data Reclassification	DCH-11	Mechanisms exist to reclassify data, including associated Technology Assets, Applications and/or Services (TAAS),	5		
MP-08(01)	Media Downgrading | Documentation of Process	Document system media downgrading actions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
MP-08(02)	Media Downgrading | Equipment Testing	Test downgrading equipment and procedures [Assignment: organization-defined frequency] to ensure that downgrading actions are being achieved.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-82 Low Overlay
MP-08(03)	Media Downgrading | Controlled Unclassified Information	Downgrade system media containing controlled unclassified information prior to public release.	Functional	Intersects With	Data Reclassification	DCH-11	Mechanisms exist to reclassify data, including associated Technology Assets, Applications and/or Services (TAAS),	5		
MP-08(04)	Media Downgrading | Classified Information	Downgrade system media containing classified information prior to release to individuals without required access authorizations.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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
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
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-01
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-02
PE-02(01)	Physical Access Authorizations | Access by Position or Role	Authorize physical access to the facility where the system resides based on position or role.	Functional	Equal	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	10		
PE-02(02)	Physical Access Authorizations | Two Forms of Identification	Require two forms of identification from the following forms of identification for visitor access to the facility where the system resides: [Assignment: organization-defined list of acceptable forms of identification].	Functional	Equal	Identification Requirement	PES-06.2	least one(1) form of government-issued or organization-issued photo identification to authenticate individuals before	10		
PE-02(03)	Physical Access Authorizations | Restrict Unescorted Access	more): security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information contained	Functional	Equal	Restrict Unescorted Access	PES-06.3	mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the	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
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-03(02)	Physical Access Control | Facility and Systems	Perform security checks [Assignment: organization-defined frequency] at the physical perimeter of the facility or system for exfiltration of information or removal of system components.	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(03)	Physical Access Control | Continuous Guards	Employ guards to control [Assignment: organization-defined physical access points] to the facility where the system resides 24 hours per day, 7 days per week.	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(04)	Physical Access Control | Lockable Casings	Use lockable physical casings to protect [Assignment: organization-defined system components] from unauthorized physical access.	Functional	Equal	Lockable Physical Casings	PES-03.2	mechanisms exist to protect system components from unauthorized physical access (e.g., lockable physical casings)	10		
PE-03(05)	Physical Access Control | Logical Tampering Protection	Employ [Assignment: organization-defined anti-tamper technologies] to [Selection (one or more): detect; prevent] physical tampering or alteration of [Assignment: organization-defined hardware components] within the system.	Functional	Equal	Mobile Device Tampering	MDM-04	through inspecting devices returning from locations that the organization deems to be of significant risk, prior to the	10		
PE-03(06)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
PE-03(07)	Physical Access Control | Physical Barriers	Limit access using physical barriers.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
PE-03(08)	Physical Access Control | Access Control Vestibules	Employ access control vestibules at [Assignment: organization-defined locations within the facility].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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-05(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
PE-05(02)	Access Control for Output Devices | Link to Individual Identity	Link individual identity to receipt of output from output devices.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
PE-05(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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
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(02)	Monitoring Physical Access | Automated Intrusion Recognition and Responses	Recognize [Assignment: organization-defined classes or types of intrusions] and initiate [Assignment: organization-defined response actions] using [Assignment: organization-defined automated	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
PE-06(03)	Monitoring Physical Access | Video Surveillance	a. Employ video surveillance of [Assignment: organization-defined operational areas];b. Review video recordings [Assignment: organization-defined frequency]; andc. Retain video recordings for [Assignment: organization-defined time period].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
PE-06(04)	Monitoring Physical Access | Monitoring Physical Access to Systems	Monitor physical access to the system in addition to the physical access monitoring of the facility at [Assignment: organization-defined physical spaces containing one or more components of the system].	Functional	Equal	Monitoring Physical Access To Critical Systems	PES-05.2	Facility security mechanisms exist to monitor physical access to critical systems or sensitive/regulated data, in	10		
PE-07		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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
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-08(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
PE-08(03)	Records | Limit Personally Identifiable Information	Limit personally identifiable information contained in visitor access records to the following elements identified in the privacy risk assessment: [Assignment: organization-defined elements].	Functional	Equal	Minimize Visitor Personal Data (PD)	PES-06.5	Mechanisms exist to minimize the collection of Personal Data (PD) contained in visitor access records.	10		
PE-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		

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	NIST SP 800-82 Low Overlay
PE-09(01)	Power Equipment and Cabling | Redundant Cabling	Employ redundant power cabling paths that are physically separated by [Assignment: organization-defined distance].	Functional	Equal	Redundant Cabling	PES-07.7	Physical security mechanisms exist to route redundant power cabling paths that are physically separated to ensure that power continues to flow in the event one of the cables is cut or otherwise	10		
PE-09(02)	Power Equipment and Cabling | Automatic Voltage Controls	Employ automatic voltage controls for [Assignment: organization-defined critical system components].	Functional	Equal	Automatic Voltage Controls	PES-07.1	Facility security mechanisms exist to utilize automatic voltage controls for critical system components.	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-10(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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-11(02)	Emergency Power | Alternate Power Supply — Self-contained	is activated [Selection (one): manually; automatically] and that is:a. Self-contained;b. Not reliant on external power generation; andc. Capable of maintaining [Selection (one): minimally required operational capability; full operational capability] in the event of an	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	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-12
PE-12(01)	Emergency Lighting | Essential Mission and Business Functions	Provide emergency lighting for all areas within the facility supporting essential mission and business functions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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
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)	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-13(02)	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	Fire Suppression Devices	PES-08.2	exist to utilize fire suppression devices/systems that provide automatic notification of any activation to organizational personnel and emergency	5		
PE-13(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
PE-13(04)	Fire Protection | Inspections	Ensure that the facility undergoes [Assignment: organization-defined frequency] fire protection inspections by authorized and qualified inspectors and identified deficiencies are resolved within [Assignment: organization-defined time period].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
PE-14	Environmental Controls	monitor, control, and maintain [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-14
PE-14(01)	Environmental Controls | Automatic Controls	Employ the following automatic environmental controls in the facility to prevent fluctuations potentially harmful to the system: [Assignment: organization-defined automatic environmental controls].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
PE-14(02)	Environmental Controls | Monitoring with Alarms and Notifications	Employ environmental control monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment to [Assignment: organization-defined personnel or roles].	Functional	Equal	Monitoring with Alarms / Notifications	PES-09.1	exist to trigger an alarm or notification of temperature and humidity changes that be potentially harmful to personnel	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
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-16
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		
PE-18(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
PE-19	Information Leakage	Protect the system from information leakage due to electromagnetic signals emanations.	Functional	Equal	Information Leakage Due To Electromagnetic Signals Emanations	PES-13	Facility security mechanisms exist to protect the system from information leakage due to electromagnetic signals emanations.	10		
PE-19(01)	Information Leakage | National Emissions Policies and Procedures	Protect system components, associated data communications, and networks in accordance with national Emissions Security policies and procedures based on the security category or classification of the information	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
PE-20	Asset Monitoring and Tracking	Employ [Assignment: organization-defined asset location technologies] to track and monitor the location and movement of [Assignment: organization-defined assets] within [Assignment: organization-defined controlled areas].	Functional	Equal	Asset Monitoring and Tracking	PES-14	technologies that track and monitor the location and movement of organization-defined assets within	10		
PE-21	Electromagnetic Pulse Protection	Employ [Assignment: organization-defined protective measures] against electromagnetic pulse damage for [Assignment: organization-defined systems and system components].	Functional	Equal	Electromagnetic Pulse (EMP) Protection	PES-15	Physical security mechanisms exist to employ safeguards against Electromagnetic Pulse (EMP) damage for systems and system components.	10		
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	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		
PE-23	Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; andb. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5		
PE-23	Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; andb. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.	Functional	Intersects With	Alternate Processing Site	BCD-09	Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.	5		
PE-23	Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; andb. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.	Functional	Intersects With	Alternate Storage Site	BCD-08	alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of	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	NIST SP 800-82 Low Overlay
PE-23	Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; andb. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.	Functional	Intersects With	Distributed Processing & Storage	SEA-15	Mechanisms exist to distribute processing and storage across multiple physical locations.	5		
PE-23	Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; andb. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.	Functional	Intersects With	Equipment Siting & Protection	PES-12	components within the facility to minimize potential damage from physical and environmental hazards and to minimize the	5		
PE-23	Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; andb. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5		
PL-01	Policy and Procedures	executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;b. Designate an [Assignment: organization-defined official] to manage	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance	10		
PL-01	Policy and Procedures	executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;b. Designate an [Assignment: organization-defined official] to manage	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
PL-01	Policy and Procedures	executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;b. Designate an [Assignment: organization-defined official] to manage	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
PL-01	Policy and Procedures	executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;b. Designate an [Assignment: organization-defined official] to manage	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
PL-01	Policy and Procedures	executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;b. Designate an [Assignment: organization-defined official] to manage	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-01
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 requirements, including a rationale for any tailoring	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
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 requirements, including a rationale for any tailoring	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
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 requirements, including a rationale for any tailoring	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-02
PL-02(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
PL-02(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
PL-02(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
PL-03		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
PL-04	Rules of Behavior	indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;c. Review and update the rules of behavior [Assignment: organization-defined frequency];and3. Require	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
PL-04	Rules of Behavior	indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;c. Review and update the rules of behavior [Assignment: organization-defined frequency];and3. Require	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
PL-04	Rules of Behavior	indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;c. Review and update the rules of behavior [Assignment: organization-defined frequency];and3. Require	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies	5		PL-04
PL-04(01)	Rules of Behavior | Social Media and External Site/application Usage Restrictions	sites/applications;b. Posting organizational information on public websites; andc. Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on	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 commercial websites and sharing	10		PL-04(01)
PL-05		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
PL-06		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
PL-07	Concept of Operations	system describing how the organization intends to operate the system from the perspective of information security and privacy; andb. Review and update the CONOPS [Assignment: organization-defined	Functional	Equal	Security Concept Of Operations (CONOPS)	OPS-02	plan for achieving cybersecurity objectives, that documents management, operational and technical measures implemented	10		
PL-08	Security and Privacy Architectures	individuals;3. Describe how the architectures are integrated into and support the enterprise architecture; and4. Describe any assumptions about, and dependencies on, external systems and services;b.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	with industry-recognized leading practices, with consideration for security, compliance and resilience principles that address risk to organizational	5		
PL-08(01)	Security and Privacy Architectures | Defense in Depth	system using a defense-in-depth approach that:a. Allocates [Assignment: organization-defined controls] to [Assignment: organization-defined locations and architectural layers]; andb. Ensures that the allocated controls operate in a coordinated and mutually	Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-03	security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality	5		
PL-08(02)	Security and Privacy Architectures | Supplier Diversity	Require that [Assignment: organization-defined controls] allocated to [Assignment: organization-defined locations and architectural layers] are obtained from different suppliers.	Functional	Intersects With	Supplier Diversity	TDA-03.1	Mechanisms exist to obtain security, compliance and resilience technologies from different suppliers to minimize supply chain risk.	5		
PL-09	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	Centralized Management of Security, Compliance & Resilience Controls	SEA-01.1	manage the organization-wide management and implementation of security, compliance and resilience	5		
PL-09	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5		
PL-09	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide	5		
PL-09	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	Centralized Management of Antimalware Technologies	END-04.3	Mechanisms exist to centrally-manage antimalware technologies.	5		
PL-09	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	Central Management	END-08.1	Mechanisms exist to centrally-manage anti-phishing and spam protection technologies.	5		
PL-09	Central Management	Centrally manage [Assignment: organization-defined controls and related processes].	Functional	Intersects With	Centralized Management of Event Log Content	MON-03.6	Mechanisms exist to centrally manage and update the criteria to be captured in event logs generated by organization-	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-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		PL-11
PM-01	Information Security Program Plan	organizational entities, and compliance;3. Reflects the coordination among organizational entities responsible for information security; and4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations	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
PM-01	Information Security Program Plan	organizational entities, and compliance;3. Reflects the coordination among organizational entities responsible for information security; and4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations	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

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	NIST SP 800-82 Low Overlay
PM-01	Information Security Program Plan	organizational entities, and compliance;3. Reflects the coordination among organizational entities responsible for information security; and4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations	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-01
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-02
PM-03	Information Security and Privacy Resources	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-03
PM-04	Plan of Action and Milestones Process	and maintained;2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and3. Are reported in accordance with	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		PM-04
PM-04	Plan of Action and Milestones Process	and maintained;2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and3. Are reported in accordance with	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	(4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection;	5		PM-04
PM-05	System Inventory	Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls	5		PM-05
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-05
PM-05(01)	System Inventory | Inventory of Personally Identifiable Information	Establish, maintain, and update [Assignment: organization-defined frequency] an inventory of all systems, applications, and projects that process personally identifiable information.	Functional	Intersects With	Inventory of Personal Data (PD)	PRI-05.5	Mechanisms exist to establish and maintain a current inventory of all Technology Assets, Applications and/or Services	5		
PM-05(01)	System Inventory | Inventory of Personally Identifiable Information	Establish, maintain, and update [Assignment: organization-defined frequency] an inventory of all systems, applications, and projects that process personally identifiable information.	Functional	Intersects With	Personal Data (PD) Inventory Automation Support	PRI-05.6	Automated mechanisms exist to determine if Personal Data (PD) is maintained in electronic form.	5		
PM-06	Measures of Performance	Develop, monitor, and report on the results of information security and privacy measures of performance.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide	5		PM-06
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-06
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 addresses risk to organizational	5		PM-07
PM-07(01)	Enterprise Architecture | Offloading	Offload [Assignment: organization-defined non-essential functions or services] to other systems, system components, or an external provider.	Functional	Equal	Outsourcing Non-Essential Functions or Services	SEA-02.2	that are capable of being outsourced to external service providers and align with the organization's enterprise	10		
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		PM-08
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-08
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-09
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-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-11
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-12
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
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-13
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
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-14
PM-15	Security and Privacy Groups and Associations	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	Threat Intelligence Program	THR-01	information-sharing capability that can influence the development of the system and security architectures, selection	5		PM-15
PM-15	Security and Privacy Groups and Associations	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-15
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-16
PM-16(01)	Threat Awareness Program | Automated Means for Sharing Threat Intelligence	Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information.	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		
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-17
PM-18	Privacy Program Plan	or 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	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-18
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-19
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

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	NIST SP 800-82 Low Overlay
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-20(01)
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-21
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 sensitive/regulated data across	5		PM-22
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-22
PM-23	Data Governance Body	Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].	Functional	Intersects With	Data Management Board	PRI-13	Mechanisms exist to establish a written charter for a Data Management Board (DMB) and assigned organization-defined roles to the DMB.	5		PM-23
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 sensitive/regulated data across	5		PM-23
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 maintained in accordance with	5		PM-23
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 maintained in accordance with	5		PM-24
PM-24	Data Integrity Board	Establish a Data Integrity Board to:a. Review proposals to conduct or participate in a matching program; andb. Conduct an annual review of all matching programs in which the agency has participated.	Functional	Intersects With	Data Management Board	PRI-13	Mechanisms exist to establish a written charter for a Data Management Board (DMB) and assigned organization-defined roles to the DMB.	5		PM-24
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 sensitive/regulated data across	5		PM-24
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
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
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		PM-24
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	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
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	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
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	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
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	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
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	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-25
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
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-26
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	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-27
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-28
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
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
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-29
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
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)
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)
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-30(01)
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-31
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		PM-32

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	NIST SP 800-82 Low Overlay
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
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
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-01
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
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-02
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-03
PS-03(01)	Personnel Screening | Classified Information	Verify that individuals accessing a system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.	Functional	Intersects With	Roles With Special Protection Measures	HRS-04.1	Individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel	5		
PS-03(02)	Personnel Screening | Formal Indoctrination	Verify that individuals accessing a system processing, storing, or transmitting types of classified information that require formal indoctrination, are formally indoctrinated for all the relevant types of information to which they have access on the system.	Functional	Equal	Formal Indoctrination	HRS-04.2	Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data	10		
PS-03(03)	Personnel Screening | Information Requiring Special Protective Measures	Verify that individuals accessing a system processing, storing, or transmitting information requiring special protection:a. Have valid access authorizations that are demonstrated by assigned official government duties; andb. Satisfy [Assignment: organization-defined	Functional	Intersects With	Roles With Special Protection Measures	HRS-04.1	Individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel	5		
PS-03(04)	Personnel Screening | Citizenship Requirements	Verify that individuals accessing a system processing, storing, or transmitting [Assignment: organization-defined information types] meet [Assignment: organization-defined citizenship requirements].	Functional	Equal	Citizenship Requirements	HRS-04.3	processing, storing, or transmitting sensitive information meet applicable statutory, regulatory and/or	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-	Functional	Equal	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	10		PS-04
PS-04(01)	Personnel Termination | Post-employment Requirements	binding post-employment requirements for the protection of organizational information; andb. Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the	Functional	Equal	Post-Employment Requirements Notification	HRS-09.3	Mechanisms exist to govern former employee behavior by formally notifying terminated individuals of their applicable,	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	a. Review and confirm ongoing operational need for current logical and physical access authorizations to system and facility when individuals are reassigned or transferred to other positions within the organization;b. Initiate [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action];c. Modify access	Functional	Equal	Personnel Transfer	HRS-08	Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or	10		PS-05
PS-06	Access Agreements	authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and3. Review and update access authorizations [Assignment: organization-defined frequency]; andc. Verify that individuals requiring access to organizational information and systems:1. Sign appropriate access agreements prior to being granted access; and2. Re-sign access agreements to	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
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		PS-06
PS-06(01)	Withdrawn		Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
PS-06(02)	Access Agreements | Classified Information Requiring Special Protection	special protection is granted only to individuals who:a. Have a valid access authorization that is demonstrated by assigned official government duties;b. Satisfy associated personnel security criteria; andc. Have	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(02)	Access Agreements | Classified Information Requiring Special Protection	special protection is granted only to individuals who:a. Have a valid access authorization that is demonstrated by assigned official government duties;b. Satisfy associated personnel security criteria; andc. Have read, understood, and signed a nondisclosure	Functional	Intersects With	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access	5		
PS-06(03)	Access Agreements | Post-employment Requirements	employment requirements for protection of organizational information; andb. Require individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered	Functional	Equal	Post-Employment Requirements Awareness	HRS-06.2	Mechanisms exist to notify individuals of their applicable, legally-binding post-employment requirements for the protection	10		
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-07
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-08
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		PS-09
PT-01	Policy and Procedures	facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;b.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient	5		
PT-01	Policy and Procedures	facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;b.	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		
PT-01	Policy and Procedures	facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;b.	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to	10		
PT-01	Policy and Procedures	facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls;b.	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		
PT-02	Authority to Process Personally Identifiable Information	organization-defined authority] that permits the [Assignment: organization-defined processing] of personally identifiable information; andb. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is	Functional	Intersects With	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store,	5		
PT-02	Authority to Process Personally Identifiable Information	[Assignment: organization-defined processing] of personally identifiable information; andb. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is	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		
PT-02	Authority to Process Personally Identifiable Information	organization-defined authority] that permits the [Assignment: organization-defined processing] of personally identifiable information; andb. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is	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		
PT-02	Authority to Process Personally Identifiable Information	organization-defined authority] that permits the [Assignment: organization-defined processing] of personally identifiable information; andb. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is	Functional	Intersects With	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the	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	NIST SP 800-82 Low Overlay
PT-02(01)	Authority to Process Personally Identifiable Information | Data Tagging	Attach data tags containing [Assignment: organization-defined authorized processing] to [Assignment: organization-defined elements of personally identifiable information].	Functional	Equal	Data Tags	DCH-22.2	Mechanisms exist to utilize data tags to automate tracking of sensitive/regulated data across the information lifecycle.	10		
PT-02(02)	Authority to Process Personally Identifiable Information | Automation	Manage enforcement of the authorized processing of personally identifiable information using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Automated Data Management Processes	PRI-02.2	Automated mechanisms exist to adjust data that is able to be collected, received, processed, stored, transmitted, shared,	5		
PT-03	Personally Identifiable Information Processing Purposes	the organization;c. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is compatible with the identified purpose(s); andd.	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		
PT-03	Personally Identifiable Information Processing Purposes	Personally identifiable information;b. Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is compatible with the identified purpose(s); andd. Monitor changes in processing personally identifiable	Functional	Intersects With	Purpose Specification	PRI-02.1	Mechanisms exist to ensure data privacy notices identify the purpose(s) for which Personal Data (PD) is collected, received,	5		
PT-03(01)	Identifiable Information Processing Purposes | Data Tagging	Attach data tags containing the following purposes to [Assignment: organization-defined elements of personally identifiable information]: [Assignment: organization-defined processing purposes].	Functional	Intersects With	Data Tagging	PRI-11	Mechanisms exist to issue data modeling guidelines to support tagging of sensitive/regulated data.	5		
PT-03(01)	Identifiable Information Processing Purposes | Data Tagging	Attach data tags containing the following purposes to [Assignment: organization-defined elements of personally identifiable information]: [Assignment: organization-defined processing purposes].	Functional	Intersects With	Data Tags	DCH-22.2	Mechanisms exist to utilize data tags to automate tracking of sensitive/regulated data across the information lifecycle.	5		
PT-03(02)	Identifiable Information Processing Purposes |	Track processing purposes of personally identifiable information using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Data Quality Automation	PRI-10.1	Automated mechanisms exist to support the evaluation of data quality across the information lifecycle.	5		
PT-03(02)	Identifiable Information Processing Purposes |	Track processing purposes of personally identifiable information using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Automated Data Management Processes	PRI-02.2	Automated mechanisms exist to adjust data that is able to be collected, received, processed, stored, transmitted, shared,	5		
PT-04	Consent	Implement [Assignment: organization-defined tools or mechanisms] for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making.	Functional	Equal	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing,	10		
PT-04(01)	Consent | Tailored Consent	Provide [Assignment: organization-defined mechanisms] to allow individuals to tailor processing permissions to selected elements of personally identifiable information.	Functional	Equal	Tailored Consent	PRI-03.1	Mechanisms exist to allow data subjects to modify permission to collect, receive, process, store, transmit, share, update and/or	10		
PT-04(02)	Consent | Just-in-time Consent	Present [Assignment: organization-defined consent mechanisms] to individuals at [Assignment: organization-defined frequency] and in conjunction with [Assignment: organization-defined personally identifiable information processing].	Functional	Intersects With	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to collect, receive, process, store,	5		
PT-04(03)	Consent | Revocation	Implement [Assignment: organization-defined tools or mechanisms] for individuals to revoke consent to the processing of their personally identifiable information.	Functional	Equal	Revoke Consent	PRI-03.4	Mechanisms exist to allow data subjects to revoke consent to collect, receive, process, store, transmit, share and/or update	10		
PT-05	Privacy Notice	organization-defined frequency];b. Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language;c. Identifies the authority that authorizes the processing	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization	5		
PT-05(01)	Privacy Notice | Just-in-time Notice	Present notice of personally identifiable information processing to individuals at a time and location where the individual provides personally identifiable information or in conjunction with a data action, or [Assignment: organization-defined frequency].	Functional	Intersects With	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to collect, receive, process, store,	5		
PT-05(02)	Privacy Notice | Privacy Act Statements	Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.	Functional	Equal	Privacy Act Statements	PRI-01.2	Data (PD); (2) Whether providing PD is mandatory or optional; (3) The principal purpose or purposes for which the PD is to	10		
PT-06	System of Records Notice	guidance and submit new and significantly modified system of records notices to the OMB and appropriate congressional committees for advance review;b. Publish system of records notices in the Federal	Functional	Equal	System of Records Notice (SORN)	PRI-02.4	Mechanisms exist to draft, publish and keep System of Records Notices (SORN) updated in accordance with regulatory guidance.	10		
PT-06(01)	System of Records Notice | Routine Uses	records notice at [Assignment: organization-defined frequency] to ensure continued accuracy, and to ensure that routine uses continue to be compatible with the purpose for which the information was	Functional	Equal	System of Records Notice (SORN) Review Process	PRI-02.5	the System of Records Notices (SORN) to ensure continued accuracy and to ensure that routine uses continue to be compatible with the purpose for	10		
PT-06(02)	System of Records Notice | Exemption Rules	system of records at [Assignment: organization-defined frequency] to ensure they remain appropriate and necessary in accordance with law, that they have been promulgated as regulations, and that they are	Functional	Equal	Privacy Act Exemptions	PRI-02.6	Mechanisms exist to review all Privacy Act exemptions claimed for the System of Records Notices (SORN) to ensure they remain appropriate and accurate	10		
PT-07	Specific Categories of Personally Identifiable Information	Apply [Assignment: organization-defined processing conditions] for specific categories of personally identifiable information.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data	5		
PT-07	Specific Categories of Personally Identifiable Information	Apply [Assignment: organization-defined processing conditions] for specific categories of personally identifiable information.	Functional	Intersects With	Personal Data (PD) Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	5		
PT-07(01)	Specific Categories of Personally Identifiable Information | Social Security Numbers	not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; andc. Inform any individual who is asked to disclose his or	Functional	Intersects With	Personal Data (PD) Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	5		
PT-07(02)	Specific Categories of Personally Identifiable Information | First Amendment	Prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.	Functional	Intersects With	Personal Data (PD) Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	5		
PT-08	Computer Matching Requirements	into a computer matching agreement;c. Publish a matching notice in the Federal Register;d. Independently verify the information produced by the matching program before taking adverse action	Functional	Intersects With	Computer Matching Agreements (CMA)	PRI-02.3	Mechanisms exist to publish Computer Matching Agreements (CMA) on the organization's public website(s).	5		
RA-01	Policy and Procedures	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
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
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-01
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-02
RA-02(01)	Security Categorization | Impact-level Prioritization	Conduct an impact-level prioritization of organizational systems to obtain additional granularity on system impact levels.	Functional	Equal	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent	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
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
RA-03(01)	Risk Assessment | Supply Chain Risk Assessment	components, and system services]; andb. 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-03(01)

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	NIST SP 800-82 Low Overlay
RA-03(02)	Risk Assessment | Use of All-source Intelligence	Use all-source intelligence to assist in the analysis of risk.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
RA-03(03)	Risk Assessment | Dynamic Threat Awareness	Determine the current cyber threat environment on an ongoing basis using [Assignment: organization-defined means].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
RA-03(04)	Risk Assessment | Predictive Cyber Analytics	Employ the following advanced automation and analytics capabilities to predict and identify risks to [Assignment: organization-defined systems or system components]: [Assignment: organization-defined advanced automation and analytics capabilities]	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
RA-04		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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
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
RA-05(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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(02)
RA-05(03)	Vulnerability Monitoring and Scanning | Breadth and Depth of Coverage	Define the breadth and depth of vulnerability scanning coverage.	Functional	Equal	Breadth / Depth of Coverage	VPM-06.2	Mechanisms exist to define the breadth and depth of coverage for vulnerability scanning that define the system components scanned and types of vulnerabilities that are checked.	10		
RA-05(04)	Vulnerability Monitoring and Scanning | Discoverable Information	Determine information about the system that is discoverable and take [Assignment: organization-defined corrective actions].	Functional	Equal	Acceptable Discoverable Information	VPM-06.8	Mechanisms exist to define what information is allowed to be discoverable by adversaries and take corrective actions to	10		
RA-05(05)	Vulnerability Monitoring and Scanning | Privileged Access	Implement privileged access authorization to [Assignment: organization-defined system components] for [Assignment: organization-defined vulnerability scanning activities].	Functional	Equal	Privileged Access	VPM-06.3	Mechanisms exist to implement privileged access authorization for selected vulnerability scanning activities.	10		
RA-05(06)	Vulnerability Monitoring and Scanning | Automated Trend Analyses	Compare the results of multiple vulnerability scans using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Trend Analysis	VPM-06.4	Automated mechanisms exist to compare the results of vulnerability scans over time to determine trends in system vulnerabilities	10		
RA-05(07)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
RA-05(08)	Vulnerability Monitoring and Scanning | Review Historic Audit Logs	Review historic audit logs to determine if a vulnerability identified in a [Assignment: organization-defined system] has been previously exploited within an [Assignment: organization-defined time period].	Functional	Equal	Review Historical Event logs	VPM-06.5	Mechanisms exist to review historical event logs to determine if identified vulnerabilities have been previously exploited.	10		
RA-05(09)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
RA-05(10)	Vulnerability Monitoring and Scanning | Correlate Scanning Information	Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors.	Functional	Equal	Correlate Scanning Information	VPM-06.9	correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack	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-05(11)
RA-06	Technical Surveillance Countermeasures Survey	survey at [Assignment: organization-defined locations] [Selection (one or more): [Assignment: organization-defined frequency]; when the following events or indicators occur: [Assignment: organization-defined	Functional	Equal	Technical Surveillance Countermeasures Security	VPM-08	Mechanisms exist to utilize a technical surveillance countermeasures survey.	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-07
RA-08	Privacy Impact Assessments	new collection of personally identifiable information that:1. Will be processed using information technology; and2. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if (determined appropriate by	Functional	Equal	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications	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		
RA-09	Criticality Analysis	identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle]	Functional	Intersects With	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality	5		
RA-09	Criticality Analysis	identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle]	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical	5		
RA-10	Threat Hunting	capability to:1. Search for indicators of compromise in organizational systems; and2. Detect, track, and disrupt threats that evade existing controls; andb. Employ the threat hunting capability [Assignment:	Functional	Equal	Threat Hunting	THR-07	cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security	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	Publishing Security, Compliance & Resilience Documentation	GOV-02	maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient	5		SA-01
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
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
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-01
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-02
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	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
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-03
SA-03(01)	System Development Life Cycle | Manage Preproduction Environment	Protect system preproduction environments commensurate with risk throughout the system development life cycle for the system, system component, or system service.	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5		
SA-03(01)	System Development Life Cycle | Manage Preproduction Environment	Protect system preproduction environments commensurate with risk throughout the system development life cycle for the system, system component, or system service.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure	5		
SA-03(01)	System Development Life Cycle | Manage Preproduction Environment	Protect system preproduction environments commensurate with risk throughout the system development life cycle for the system, system component, or system service.	Functional	Intersects With	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	5		

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	NIST SP 800-82 Low Overlay
SA-03(02)	System Development Life Cycle | Use of Live or Operational Data	in preproduction environments for the system; system component, or system service; andb. Protect preproduction environments for the system, system component, or system service at the same impact or classification level as any live data in use within the	Functional	Equal	Use of Live Data	TDA-10	Mechanisms exist to approve, document and control the use of live data in development and test environments.	10		
SA-03(03)	System Development Life Cycle | Technology Refresh	Plan for and implement a technology refresh schedule for the system throughout the system development life cycle.	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5		
SA-03(03)	System Development Life Cycle | Technology Refresh	Plan for and implement a technology refresh schedule for the system throughout the system development life cycle.	Functional	Intersects With	Refresh from Trusted Sources	SEA-08.1	Mechanisms exist to ensure that software and data needed for system component and service refreshes are obtained from	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
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
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
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		SA-04
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	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	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	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(03)	Acquisition Process | Development Methods, Techniques, and Practices	includes:a. [Assignment: organization-defined systems engineering methods];b. [Assignment: organization-defined [Selection (one or more): systems security; privacy] engineering methods]; andc. [Assignment:	Functional	Intersects With	Development Methods, Techniques & Processes	TDA-02.3	processes employ industry-recognized secure practices for secure programming, engineering methods, quality	5		
SA-04(03)	Acquisition Process | Development Methods, Techniques, and Practices	includes:a. [Assignment: organization-defined systems engineering methods];b. [Assignment: organization-defined [Selection (one or more): systems security; privacy] engineering methods]; andc. [Assignment:	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		
SA-04(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-04(05)	Acquisition Process | System, Component, and Service Configurations	component, or system service to:a. Deliver the system, component, or service with [Assignment: organization-defined security configurations] implemented; andb. Use the configurations as the default for any subsequent system, component, or service	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(06)	Acquisition Process | Use of Information Assurance Products	that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; andb.	Functional	Equal	Commercial Off-The-Shelf (COTS) Security Solutions	TDA-03	Mechanisms exist to utilize only Commercial Off-the-Shelf (COTS) security products.	10		
SA-04(07)	Acquisition Process | NIAP-approved Protection Profiles	Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; andb. Require, if no NIAP-approved Protection Profile exists for a specific technology type	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(08)	Acquisition Process | Continuous Monitoring Plan for Controls	Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of control effectiveness that is consistent with the continuous monitoring program of the organization	Functional	Equal	Continuous Monitoring Plan	TDA-09.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a plan for the	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(10)
SA-04(11)	Acquisition Process | System of Records	include [Assignment: organization-defined Privacy Act requirements] in the acquisition contract for the operation of a system of records on behalf of an organization to accomplish an organizational mission	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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)
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)
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-04(12)
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
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-05
SA-05(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-05(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-05(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-05(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-05(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-06		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-07		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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
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-08
SA-08(01)	Security and Privacy Engineering Principles | Clear Abstractions	Implement the security design principle of clear abstractions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-82 Low Overlay
SA-08(02)	Security and Privacy Engineering Principles | Least Common Mechanism	Implement the security design principle of least common mechanism in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(03)	Security and Privacy Engineering Principles | Modularity and Layering	Implement the security design principles of modularity and layering in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(04)	Security and Privacy Engineering Principles | Partially Ordered Dependencies	Implement the security design principle of partially ordered dependencies in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(05)	Security and Privacy Engineering Principles | Efficiently Mediated Access	Implement the security design principle of efficiently mediated access in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(06)	Security and Privacy Engineering Principles | Minimized Sharing	Implement the security design principle of minimized sharing in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(07)	Security and Privacy Engineering Principles | Reduced Complexity	Implement the security design principle of reduced complexity in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(08)	Security and Privacy Engineering Principles | Secure Evolvability	Implement the security design principle of secure evolvability in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(09)	Security and Privacy Engineering Principles | Trusted Components	Implement the security design principle of trusted components in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(10)	Security and Privacy Engineering Principles | Hierarchical Trust	Implement the security design principle of hierarchical trust in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(11)	Security and Privacy Engineering Principles | Inverse Modification Threshold	Implement the security design principle of inverse modification threshold in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(12)	Security and Privacy Engineering Principles | Hierarchical Protection	Implement the security design principle of hierarchical protection in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(13)	Security and Privacy Engineering Principles | Minimized Security Elements	Implement the security design principle of minimized security elements in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(14)	Security and Privacy Engineering Principles | Least Privilege	Implement the security design principle of least privilege in [Assignment: organization-defined systems or system components].	Functional	Equal	Least Privilege	IAC-21	concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational	10		
SA-08(15)	Security and Privacy Engineering Principles | Predicate Permission	Implement the security design principle of predicate permission in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(16)	Security and Privacy Engineering Principles | Self-reliant Trustworthiness	Implement the security design principle of self-reliant trustworthiness in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(17)	Security and Privacy Engineering Principles | Secure Distributed Composition	Implement the security design principle of secure distributed composition in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(18)	Security and Privacy Engineering Principles | Trusted Communications Channels	Implement the security design principle of trusted communications channels in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(19)	Security and Privacy Engineering Principles | Continuous Protection	Implement the security design principle of continuous protection in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(20)	Security and Privacy Engineering Principles | Secure Metadata Management	Implement the security design principle of secure metadata management in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(21)	Security and Privacy Engineering Principles | Self-analysis	Implement the security design principle of self-analysis in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(22)	Security and Privacy Engineering Principles | Accountability and Traceability	Implement the security design principle of accountability and traceability in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(23)	Security and Privacy Engineering Principles | Secure Defaults	Implement the security design principle of secure defaults in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(24)	Security and Privacy Engineering Principles | Secure Failure and Recovery	Implement the security design principle of secure failure and recovery in [Assignment: organization-defined systems or system components].	Functional	Equal	Fail Secure	SEA-07.2	systems to fail to an organization-defined known-state for types of failures, preserving system state information in	10		
SA-08(25)	Security and Privacy Engineering Principles | Economic Security	Implement the security design principle of economic security in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(26)	Security and Privacy Engineering Principles | Performance Security	Implement the security design principle of performance security in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(27)	Security and Privacy Engineering Principles | Human Factored Security	Implement the security design principle of human factored security in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(28)	Security and Privacy Engineering Principles | Acceptable Security	Implement the security design principle of acceptable security in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(29)	Privacy Engineering Principles | Repeatable and Documented	Implement the security design principle of repeatable and documented procedures in [Assignment: organization-defined systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-08(30)	Security and Privacy Engineering Principles | Procedural Rigor	Implement the security design principle of procedural rigor in [Assignment: organization-defined systems or system components].	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure	5		
SA-08(30)	Security and Privacy Engineering Principles | Procedural Rigor	Implement the security design principle of procedural rigor in [Assignment: organization-defined systems or system components].	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5		
SA-08(31)	Security and Privacy Engineering Principles | Secure System Modification	Implement the security design principle of secure system modification in [Assignment: organization-defined systems or system components].	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5		

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	NIST SP 800-82 Low Overlay
SA-08(31)	Security and Privacy Engineering Principles | Secure System Modification	Implement the security design principle of secure system modification in [Assignment: organization-defined systems or system components].	Functional	Intersects With	Control Functionality Verification	CHG-06	functionality of security, compliance and resilience controls following implemented changes to ensure applicable	5		
SA-08(31)	Security and Privacy Engineering Principles | Secure System Modification	Implement the security design principle of secure system modification in [Assignment: organization-defined systems or system components].	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	appropriately test and document proposed changes in a non-production environment before changes are implemented in a	5		
SA-08(32)	Security and Privacy Engineering Principles | Sufficient Documentation	Implement the security design principle of sufficient documentation in [Assignment: organization-defined systems or system components].	Functional	Equal	Standardized Operating Procedures (SOP)	OPS-01.1	document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-	10		
SA-08(33)	Security and Privacy Engineering Principles | Minimization	Implement the privacy principle of minimization using [Assignment: organization-defined processes].	Functional	Intersects With	Collection Minimization	END-13.3	Mechanisms exist to utilize sensors that are configured to minimize the collection of information about individuals.	5		
SA-08(33)	Security and Privacy Engineering Principles | Minimization	Implement the privacy principle of minimization using [Assignment: organization-defined processes].	Functional	Intersects With	Limit Sensitive / Regulated Data In Testing, Training & Research	DCH-18.2	the use of sensitive/regulated data for research, testing, or training, in accordance with authorized, legitimate business	5		
SA-08(33)	Security and Privacy Engineering Principles | Minimization	Implement the privacy principle of minimization using [Assignment: organization-defined processes].	Functional	Intersects With	Minimize Visitor Personal Data (PD)	PES-06.5	Mechanisms exist to minimize the collection of Personal Data (PD) contained in visitor access records.	5		
SA-09	External System Services	[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
SA-09(01)	External System Services | Risk Assessments and Organizational Approvals	to the acquisition or outsourcing of information security services; andb. Verify that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined	Functional	Equal	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology	10		
SA-09(02)	External System Services | Identification of Functions, Ports, Protocols, and Services	Require providers of the following 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-09(03)	External System Services | Establish and Maintain Trust Relationship with Providers	with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions	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		
SA-09(03)	External System Services | Establish and Maintain Trust Relationship with Providers	with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions	Functional	Intersects With	Conflict of Interests	TPM-04.3	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	5		
SA-09(03)	External System Services | Establish and Maintain Trust Relationship with Providers	with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions	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-09(03)	External System Services | Establish and Maintain Trust Relationship with Providers	with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions	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		
SA-09(03)	External System Services | Establish and Maintain Trust Relationship with Providers	with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions	Functional	Intersects With	Accountable, Supportive, Consulted & Informed (RASCI)	TPM-05.4	consulted & informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between	5		
SA-09(03)	External System Services | Establish and Maintain Trust Relationship with Providers	with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions	Functional	Intersects With	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance	5		
SA-09(04)	External System Services | Consistent Interests of Consumers and Providers	Take the following actions to verify that the interests of [Assignment: organization-defined external service providers] are consistent with and reflect organizational interests: [Assignment: organization-defined actions]	Functional	Equal	Conflict of Interests	TPM-04.3	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	10		
SA-09(05)	External System Services | Processing, Storage, and Service Location	Restrict the location of [Selection (one or more): information processing; information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	location of cloud processing/storage based on business requirements that includes statutory, regulatory	5		
SA-09(05)	External System Services | Processing, Storage, and Service Location	Restrict the location of [Selection (one or more): information processing; information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5		
SA-09(05)	External System Services | Processing, Storage, and Service Location	Restrict the location of [Selection (one or more): information processing; information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].	Functional	Intersects With	Geographic Location of Data	DCH-19	flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure	5		
SA-09(06)	External System Services | Organization-controlled Cryptographic Keys	Maintain exclusive control of cryptographic keys for encrypted material stored or transmitted through an external system.	Functional	Equal	External System Cryptographic Key Control	CRY-09.7	mechanisms exist to maintain control of cryptographic keys for encrypted material stored or transmitted through an external system	10		
SA-09(07)	External System Services | Organization-controlled Integrity Checking	Provide the capability to check the integrity of information while it resides in the external system.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-09(08)	External System Services | Processing and Storage Location — U.S. Jurisdiction	Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States.	Functional	Intersects With	Geographic Location of Data	DCH-19	flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure	5		
SA-09(08)	External System Services | Processing and Storage Location — U.S. Jurisdiction	Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	location of cloud processing/storage based on business requirements that includes statutory, regulatory	5		
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-10(01)	Configuration Management | Software and Firmware Integrity	Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components.	Functional	Equal	Software / Firmware Integrity Verification	TDA-14.1	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity	10		
SA-10(02)	Configuration Management | Alternative Configuration Management	Provide an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-10(03)	Developer Configuration Management | Hardware Integrity Verification	Require the developer of the system, system component, or system service to enable integrity verification of hardware components.	Functional	Equal	Hardware Integrity Verification	TDA-14.2	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity	10		
SA-10(04)	Developer Configuration Management | Trusted Generation	Require the developer of the system, system component, or system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions, source code, and object code with previous versions	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-10(05)	Developer Configuration Management | Mapping Integrity for Version Control	component, or system service to maintain the integrity of the mapping between the master build data describing the current version of security-relevant hardware, software, and firmware and the on-site	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-10(06)	Developer Configuration Management | Trusted Distribution	Require the developer of the system, system component, or system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-10(07)	Configuration Management | Security and Privacy	Require [Assignment: organization-defined security and privacy representatives] to be included in the [Assignment: organization-defined configuration change management and control process].	Functional	Equal	Security, Compliance & Resilience Representatives For Product Changes	TDA-02.7	appropriate security, compliance and resilience representatives in the product feature and/or functionality change control	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	NIST SP 800-82 Low Overlay
SA-11	Developer Testing and Evaluation	and privacy control assessments;b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency] at [Assignment: organization-defined depth and coverage];c. Produce evidence of the execution of	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-11(01)	Developer Testing and Evaluation | Static Code Analysis	Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.	Functional	Equal	Static Code Analysis	TDA-09.2	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ static code	10		
SA-11(02)	Developer Testing and Evaluation | Threat Modeling and Vulnerability Analyses	[Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels];b. Employs the following tools and methods: [Assignment: organization-defined information	Functional	Intersects With	reat Analysis & Flaw	TDA-15	integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and	5		
SA-11(02)	Developer Testing and Evaluation | Threat Modeling and Vulnerability Analyses	concerning impact, environment of operations, known or assumed threats, and acceptable risk levels];b. Employs the following tools and methods: [Assignment: organization-defined tools and	Functional	Intersects With	Threat Modeling	TDA-06.2	threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and	5		
SA-11(03)	Developer Testing and Evaluation | Independent Verification of Assessment Plans	criteria];b. Verify the correct implementation of the developer security and privacy assessment plans and the evidence produced during testing and evaluation; andb. Verify that the independent agent is provided with sufficient information to complete the verification	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-11(04)	Developer Testing and Evaluation | Manual Code Reviews	code review of [Assignment: organization-defined specific code] using the following processes, procedures, and/or techniques: [Assignment: organization-defined processes, procedures, and/or	Functional	Equal	Manual Code Review	TDA-09.7	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ a manual code	10		
SA-11(05)	Developer Testing and Evaluation | Penetration Testing	component, or system service to perform penetration testing:a. At the following level of rigor: [Assignment: organization-defined breadth and depth of testing]; andb. Under the following constraints: [Assignment:	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws	5		
SA-11(05)	Developer Testing and Evaluation | Penetration Testing	component, or system service to perform penetration testing:a. At the following level of rigor: [Assignment: organization-defined breadth and depth of testing]; andb. Under the following constraints: [Assignment:	Functional	Intersects With	Application Penetration Testing	TDA-09.5	Mechanisms exist to perform application-level penetration testing of custom-made Technology Assets, Applications	5		
SA-11(05)	Developer Testing and Evaluation | Penetration Testing	component, or system service to perform penetration testing:a. At the following level of rigor: [Assignment: organization-defined breadth and depth of testing]; andb. Under the following constraints: [Assignment:	Functional	Intersects With	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	5		
SA-11(05)	Developer Testing and Evaluation | Penetration Testing	component, or system service to perform penetration testing:a. At the following level of rigor: [Assignment: organization-defined breadth and depth of testing]; andb. Under the following constraints: [Assignment:	Functional	Intersects With	Specialized Assessments	IAO-02.2	(4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.);	5		
SA-11(05)	Developer Testing and Evaluation | Penetration Testing	component, or system service to perform penetration testing:a. At the following level of rigor: [Assignment: organization-defined breadth and depth of testing]; andb. Under the following constraints: [Assignment:	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5		
SA-11(06)	Developer Testing and Evaluation | Attack Surface Reviews	Require the developer of the system, system component, or system service to perform attack surface reviews.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct	5		
SA-11(06)	Developer Testing and Evaluation | Attack Surface Reviews	Require the developer of the system, system component, or system service to perform attack surface reviews.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5		
SA-11(07)	Developer Testing and Evaluation | Verify Scope of Testing and Evaluation	component, or system service to verify that the scope of testing and evaluation provides complete coverage of the required controls at the following level of rigor: [Assignment: organization-defined breadth and depth	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5		
SA-11(07)	Developer Testing and Evaluation | Verify Scope of Testing and Evaluation	component, or system service to verify that the scope of testing and evaluation provides complete coverage of the required controls at the following level of rigor: [Assignment: organization-defined breadth and depth	Functional	Intersects With	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	5		
SA-11(08)	Developer Testing and Evaluation | Dynamic Code Analysis	Require the developer of the system, system component, or system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.	Functional	Equal	Dynamic Code Analysis	TDA-09.3	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ dynamic code	10		
SA-11(09)	Developer Testing and Evaluation | Interactive Application Security Testing	Require the developer of the system, system component, or system service to employ interactive application security testing tools to identify flaws and document the results.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-12		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-12(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-12(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-12(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-12(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-12(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-12(06)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-12(07)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-12(08)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-12(09)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-12(10)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-12(11)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-12(12)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-12(13)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-12(14)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-12(15)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-13		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-14		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-14(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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(01)	Development Process, Standards, and Tools | Quality Metrics	component, or system service:a. At the beginning of the development process; andb. Provide evidence of meeting the quality metrics [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-15(02)	Development Process, Standards, and Tools | Security and Privacy Tracking Tools	Require the developer of the system, system component, or system service to select and employ security and privacy tracking tools for use during the development process.	Functional	Equal	Capabilities Deficiency Tracking	IAO-05	(4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection;	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-15(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-15(05)	Development Process, Standards, and Tools | Attack Surface Reduction	Require the developer of the system, system component, or system service to reduce attack surfaces to [Assignment: organization-defined thresholds].	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications	5		
SA-15(05)	Development Process, Standards, and Tools | Attack Surface Reduction	Require the developer of the system, system component, or system service to reduce attack surfaces to [Assignment: organization-defined thresholds].	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the	5		
SA-15(06)	Development Process, Standards, and Tools | Continuous Improvement	Require the developer of the system, system component, or system service to implement an explicit process to continuously improve the development process.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-15(07)	Process, Standards, and Tools | Automated Vulnerability	automated vulnerability analysis using [Assignment: organization-defined tools];b. Determine the exploitation potential for discovered vulnerabilities;c. Determine potential risk mitigations for delivered	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-82 Low Overlay
SA-15(08)	Process, Standards, and Tools | Reuse of Threat and Vulnerability	Require the developer of the system, system component, or system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process.	Functional	Equal	Threat Modeling	TDA-06.2	threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and	10		
SA-15(09)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-15(10)	Development Process, Standards, and Tools | Incident Response Plan	Require the developer of the system, system component, or system service to provide, implement, and test an incident response plan.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-15(11)	Development Process, Standards, and Tools | Archive System or Component	Require the developer of the system or system component to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security and privacy review.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-15(12)	Process, Standards, and Tools | Minimize Personally Identifiable	Require the developer of the system or system component to minimize the use of personally identifiable information in development and test environments.	Functional	Equal	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	10		
SA-15(13)	Development Process, Standards, and Tools | Logging Syntax	Require the developer of the system, system component, or system service to use [Assignment: organization-defined secure logging format] to log [assignment: organization-defined event types] at [assignment: organization-defined level of detail].	Functional	Equal	Logging Syntax	TDA-02.14	Mechanisms exist to require system developers to use an industry-defined secure logging format to generate event logs for	10		
SA-16	Developer-provided Training	Require the developer of the system, system component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: [Assignment: organization-defined	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	Require the developer of the system, system component, or system service to produce a 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-17(01)	Developer Security and Privacy Architecture and Design | Formal Policy Model	Require the developer of the system, system component, or system service to produce, and update as necessary, a formal policy model describing the [Assignment: organization-defined elements of organizational security and privacy policy] to be enforced; andb. Prove that the formal policy model is internally consistent and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-17(02)	Developer Security and Privacy Architecture and Design | Security-relevant Components	Require the developer of the system, system component, or system service to:a. Define security-relevant hardware, software, and firmware; andb. Provide a rationale that the definition for security-relevant hardware, software, and firmware is	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-17(03)	Developer Security and Privacy Architecture and Design | Formal Correspondence	Require the developer of the system, system component, or system service to produce a formal top-level specification that is consistent with the formal policy model;c. Show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware, software,	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-17(04)	Developer Security and Privacy Architecture and Design | Informal Correspondence	Require the developer of the system, system component, or system service to produce a descriptive top-level specification and [Selection (one or more): informal demonstration; [Assignment: organization-defined	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-17(05)	Developer Security and Privacy Architecture and Design | Conceptually Simple Design	Require the developer of the system, system component, or system service to describe the conceptual design of the security-relevant hardware, software, and firmware that: a. Is consistent with the security architecture; b. Describes how the security-relevant hardware, software, and firmware to use a complete, conceptually simple protection mechanism with precisely defined semantics; andb. Internally structure the security-	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-17(06)	Developer Security and Privacy Architecture and Design | Structure for Testing	Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate testing.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-17(07)	Developer Security and Privacy Architecture and Design | Structure for Least Privilege	Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-17(08)	Developer Security and Privacy Architecture and Design | Orchestration	Design [Assignment: organization-defined critical systems or system components] with coordinated behavior to implement the following capabilities: [Assignment: organization-defined capabilities, by system or component].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-17(09)	Developer Security and Privacy Architecture and Design | Design Diversity	Use different designs for [Assignment: organization-defined critical systems or system components] to satisfy a common set of requirements or to provide equivalent functionality.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SA-18		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-18(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-18(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-19		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-19(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-19(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-19(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-19(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-20	Customized Development of Critical Components	Reimplement or custom develop the following critical system components: [Assignment: organization-defined critical system components].	Functional	Equal	Customized Development of Critical Components	TDA-12	Mechanisms exist to custom-develop critical system components, when Commercial Off The Shelf (COTS) solutions are unavailable.	10		
SA-21	Developer Screening	Require that the developer of [Assignment: organization-defined system or system component] [Selection (one or more): have an access authorization; reside in [Assignment: organization-defined	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-21(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-22	Unsupported System Components	Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; orb. Provide the following options for alternative sources for continued support for unsupported components [Selection (one or more): in-house support; [Assignment: organization-defined	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
SA-22	Unsupported System Components	Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; orb. Provide the following options for alternative sources for continued support for unsupported components [Selection (one or more): in-house support; [Assignment: organization-defined	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		SA-22
SA-22(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SA-23	Specialization	Specialize [Assignment: organization-defined system or system component] by [Selection (one or more): performing a specific mission function or service; hosting [Assignment: organization-defined	Functional	Intersects With	Technology Development & Acquisition	TDA-01	implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet	5		
SA-23	Specialization	Specialize [Assignment: organization-defined system or system component] by [Selection (one or more): performing a specific mission function or service; hosting [Assignment: organization-defined	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and	5		
SA-23	Specialization	Specialize [Assignment: organization-defined system or system component] by [Selection (one or more): performing a specific mission function or service; hosting [Assignment: organization-defined	Functional	Intersects With	Customized Development of Critical Components	TDA-12	Mechanisms exist to custom-develop critical system components, when Commercial Off The Shelf (COTS) solutions are unavailable.	5		
SC-01	Policy and Procedures	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: [Selection (one or more): organization-level; mission/business process-level; system-level] [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		SC-01
SC-01	Policy and Procedures	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: [Selection (one or more): organization-level; mission/business process-level; system-level] [Assignment: organization-defined	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
SC-01	Policy and Procedures	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: [Selection (one or more): organization-level; mission/business process-level; system-level] [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		SC-01
SC-01	Policy and Procedures	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: [Selection (one or more): organization-level; mission/business process-level; system-level] [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		SC-01
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		

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	NIST SP 800-82 Low Overlay
SC-02(01)	Separation of System and User Functionality | Interfaces for Non-privileged Users	Prevent the presentation of system management functionality at interfaces to non-privileged users.	Functional	Equal	Application Partitioning	SEA-03.2	Mechanisms exist to separate user functionality from system management functionality.	10		
SC-02(02)	Separation of System and User Functionality | Disassociability	Store state information from applications and software separately.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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-03(01)	Security Function Isolation | Hardware Separation	Employ hardware separation mechanisms to implement security function isolation.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-03(02)	Security Function Isolation | Access and Flow Control Functions	Isolate security functions enforcing access and information flow control from nonsecurity functions and from other security functions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-03(03)	Security Function Isolation | Minimize Nonsecurity Functionality	Minimize the number of nonsecurity functions included within the isolation boundary containing security functions.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-03(04)	Security Function Isolation | Module Coupling and Cohesiveness	Implement security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-03(05)	Security Function Isolation | Layered Structures	Implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	Functional	Equal	Defense-In-Depth (DiD) Architecture	SEA-03	security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality	10		
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-04(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SC-04(02)	Information in Shared System Resources | Multilevel or Periods Processing	Prevent unauthorized information transfer via shared resources in accordance with [Assignment: organization-defined procedures] when system processing explicitly switches between different information classification levels or security categories	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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
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
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
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-05
SC-05(01)	Denial-of-service Protection | Restrict Ability to Attack Other Systems	Restrict the ability of individuals to launch the following denial-of-service attacks against other systems: [Assignment: organization-defined denial-of-service attacks].	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are	5		
SC-05(02)	Denial-of-service Protection | Capacity, Bandwidth, and Redundancy	Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks.	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are	5		
SC-05(02)	Denial-of-service Protection | Capacity, Bandwidth, and Redundancy	Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks.	Functional	Intersects With	Capacity Planning	CAP-03	capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist	5		
SC-05(03)	Denial-of-service Protection | Detection and Monitoring	indicators of denial-of-service attacks against, or launched from, the system: [Assignment: organization-defined monitoring tools]; andb. Monitor the following system resources to determine if sufficient resources exist to prevent effective denial-of-service attacks:	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-06	Resource Availability	Protect the availability of resources by allocating [Assignment: organization-defined resources] by [Selection (one or more): priority; quota; [Assignment: organization-defined controls]].	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-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
SC-07(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SC-07(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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(06)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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(09)	Protection | Restrict Threatening Outgoing Communications	a. Detect and deny outgoing communications traffic posing a threat to external systems; andb. Audit the identity of internal users associated with denied communications.	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network	5		
SC-07(09)	Protection | Restrict Threatening Outgoing Communications	a. Detect and deny outgoing communications traffic posing a threat to external systems; andb. Audit the identity of internal users associated with denied communications.	Functional	Intersects With	External Telecommunications Services	NET-03.2	external telecommunication service that protects the confidentiality and integrity of the information being	5		
SC-07(10)	Boundary Protection | Prevent Exfiltration	a. Prevent the exfiltration of information; andb. Conduct exfiltration tests [Assignment: organization-defined frequency].	Functional	Intersects With	Prevent Unauthorized Exfiltration	NET-03.5	Automated mechanisms exist to prevent the unauthorized exfiltration of sensitive/regulated data across managed interfaces.	5		

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	NIST SP 800-82 Low Overlay
SC-07(10)	Boundary Protection | Prevent Exfiltration	a. Prevent the exfiltration of information; andb. Conduct exfiltration tests [Assignment: organization-defined frequency].	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5		
SC-07(11)	Boundary Protection | Restrict Incoming Communications Traffic	Only allow incoming communications from [Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized destinations].	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit	5		
SC-07(11)	Boundary Protection | Restrict Incoming Communications Traffic	Only allow incoming communications from [Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized destinations].	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5		
SC-07(12)	Boundary Protection | Host-based Protection	Implement [Assignment: organization-defined host-based boundary protection mechanisms] at [Assignment: organization-defined system components].	Functional	Equal	Host-Based Security Function Isolation	END-16.1	Mechanisms exist to implement underlying software separation mechanisms to facilitate security function isolation.	10		
SC-07(13)	Protection | Isolation of Security Tools, Mechanisms, and Support	security tools, mechanisms, and support components] from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the	Functional	Intersects With	Security Management Subnets	NET-06.1	Isolate security tools and support components from other internal system components by implementing separate subnetworks with managed	5		
SC-07(14)	Protection | Protect Against Unauthorized Physical	Protect against unauthorized physical connections at [Assignment: organization-defined managed interfaces].	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		
SC-07(14)	Protection | Protect Against Unauthorized Physical	Protect against unauthorized physical connections at [Assignment: organization-defined managed interfaces].	Functional	Intersects With	Lockable Physical Casings	PES-03.2	Physical access control mechanisms exist to protect system components from unauthorized physical access (e.g., lockable cabinets)	5		
SC-07(14)	Protection | Protect Against Unauthorized Physical	Protect against unauthorized physical connections at [Assignment: organization-defined managed interfaces].	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical access control mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or	5		
SC-07(15)	Boundary Protection | Networked Privileged Accesses	Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.	Functional	Equal	Route Privileged Network Access	NET-18.3	Automated mechanisms exist to route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.	10		
SC-07(16)	Boundary Protection | Prevent Discovery of System Components	Prevent the discovery of specific system components that represent a managed interface.	Functional	Equal	Prevent Discovery of Internal Information	NET-03.3	Mechanisms exist to prevent the public disclosure of internal network information.	10		
SC-07(17)	Boundary Protection | Automated Enforcement of Protocol Formats	Enforce adherence to protocol formats.	Functional	Equal	Web Application Firewall (WAF)	WEB-03	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.	10		
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(19)	Protection | Block Communication from Non-organizationally	Block inbound and outbound communications traffic between [Assignment: organization-defined communication clients] that are independently configured by end users and external service providers.	Functional	Intersects With	Network Access Control (NAC)	AST-02.5	employ network access control (NAC), or a similar technology, which is capable of detecting unauthorized devices and disable network access to those	5		
SC-07(20)	Boundary Protection | Dynamic Isolation and Segregation	Provide the capability to dynamically isolate [Assignment: organization-defined system components] from other system components.	Functional	Equal	Dynamic Isolation & Segregation (Sandboxing)	NET-03.6	sandbox) untrusted components during runtime, where the component is isolated in a fault-contained environment but it can	10		
SC-07(21)	Boundary Protection | Isolation of System Components	Employ boundary protection mechanisms to isolate [Assignment: organization-defined system components] supporting [Assignment: organization-defined missions and/or business functions].	Functional	Equal	Isolation of System Components	NET-03.7	Mechanisms exist to employ boundary protections to isolate Technology Assets, Applications and/or Services (TAAS) that	10		
SC-07(22)	Protection | Separate Subnets for Connecting to Different Security	Implement separate network addresses to connect to systems in different security domains.	Functional	Intersects With	Separate Subnet for Connecting to Different Security Domains	NET-03.8	Mechanisms exist to implement separate network addresses (e.g., different subnets) to connect to systems in different security domains.	5		
SC-07(23)	Boundary Protection | Disable Sender Feedback on Protocol Validation Failure	Disable feedback to senders on protocol format validation failure.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-07(24)	Boundary Protection | Personally Identifiable Information	data elements of personally identifiable information: [Assignment: organization-defined processing rules];b. Monitor for permitted processing at the external interfaces to the system and at key internal boundaries	Functional	Equal	Personal Data (PD)	NET-03.4	Mechanisms exist to apply network-based processing rules to data elements of Personal Data (PD).	10		
SC-07(25)	Protection | Unclassified National Security System	Prohibit the direct connection of [Assignment: organization-defined unclassified national security system] to an external network without the use of [Assignment: organization-defined boundary protection device].	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics;	5		
SC-07(26)	Boundary Protection | Classified National Security System Connections	Prohibit the direct connection of a classified national security system to an external network without the use of [Assignment: organization-defined boundary protection device].	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics;	5		
SC-07(27)	Protection | Unclassified Non-national Security System	Prohibit the direct connection of [Assignment: organization-defined unclassified non-national security system] to an external network without the use of [Assignment: organization-defined boundary protection device].	Functional	Equal	External System Connections	NET-05.1	direct connection of a sensitive system to an external network without the use of an organization-defined boundary	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(28)
SC-07(29)	Boundary Protection | Separate Subnets to Isolate Functions	Implement [Selection (one): physically; logically] separate subnetworks to isolate the following critical system components and functions: [Assignment: organization-defined critical system components and functions].	Functional	Intersects With	Cloud Infrastructure Security Subnet	CLD-03	Mechanisms exist to host security-specific technologies in a dedicated subnet.	5		SC-07(29)
SC-07(29)	Boundary Protection | Separate Subnets to Isolate Functions	Implement [Selection (one): physically; logically] separate subnetworks to isolate the following critical system components and functions: [Assignment: organization-defined critical system components and functions].	Functional	Intersects With	Security Management Subnets	NET-06.1	Isolate security tools and support components from other internal system components by implementing separate subnetworks with managed	5		
SC-07(29)	Boundary Protection | Separate Subnets to Isolate Functions	Implement [Selection (one): physically; logically] separate subnetworks to isolate the following critical system components and functions: [Assignment: organization-defined critical system components and functions].	Functional	Intersects With	Separate Subnet for Connecting to Different Security Domains	NET-03.8	Mechanisms exist to implement separate network addresses (e.g., different subnets) to connect to systems in different security domains.	5		
SC-08	Transmission Confidentiality and Integrity	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5		
SC-08	Transmission Confidentiality and Integrity	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5		
SC-08(01)	Transmission Confidentiality and Integrity | Cryptographic Protection	Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	Functional	Intersects With	Alternate Physical Protection	CRY-01.1	Cryptographic mechanisms exist to prevent unauthorized disclosure of information as an alternative to physical safeguards.	5		
SC-08(01)	Transmission Confidentiality and Integrity | Cryptographic Protection	Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5		
SC-08(01)	Transmission Confidentiality and Integrity | Cryptographic Protection	Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5		
SC-08(02)	Transmission Confidentiality and Integrity | Pre- and Post-transmission Handling	Maintain the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.	Functional	Intersects With	Pre/Post Transmission Handling	CRY-01.3	Cryptographic mechanisms exist to ensure the confidentiality and integrity of information during preparation for transmission and during reception.	5		

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	NIST SP 800-82 Low Overlay
SC-08(02)	Transmission Confidentiality and Integrity | Pre- and Post-transmission Handling	Maintain the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5		
SC-08(02)	Transmission Confidentiality and Integrity | Pre- and Post-transmission Handling	Maintain the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.	Functional	Intersects With	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5		
SC-08(03)	Confidentiality and Integrity | Cryptographic Protection for Transmission	Implement cryptographic mechanisms to protect message externals unless otherwise protected by [Assignment: organization-defined alternative physical controls].	Functional	Equal	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	10		
SC-08(04)	Transmission Confidentiality and Integrity | Conceal or Randomize Communications	Implement cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by [Assignment: organization-defined alternative physical controls].	Functional	Equal	Conceal / Randomize Communications	CRY-01.4	Cryptographic mechanisms exist to conceal or randomize communication patterns.	10		
SC-08(05)	Transmission Confidentiality and Integrity | Protected Distribution System	Implement [Assignment: organization-defined protected distribution system] to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-09		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SC-10	Network Disconnect	Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.	Functional	Equal	Network Connection Termination	NET-07	Mechanisms exist to terminate network connections at the end of a session or after an organization-defined time period of inactivity.	10		
SC-11	Trusted Path	communications between the user and the trusted components of the system; andb. Permit users to invoke the trusted communications path for communications between the user and the following security functions of the system, including at a	Functional	Equal	Trusted Path	END-09	Mechanisms exist to establish a trusted communications path between the user and the security functions of the operating system.	10		
SC-11(01)	Trusted Path | Irrefutable Communications Path	irrefutably distinguishable from other communications paths; andb. Initiate the trusted communications path for communications between the [Assignment: organization-defined security functions] of the system	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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
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-12(02)	Cryptographic Key Establishment and Management | Symmetric Keys	Produce, control, and distribute symmetric cryptographic keys using [Selection (one): NIST FIPS-validated; NSA-approved] key management technology and processes.	Functional	Equal	Symmetric Keys	CRY-09.1	Facilitate the production and management of symmetric cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key management	10		
SC-12(03)	Cryptographic Key Establishment and Management | Asymmetric Keys	approved key management technology and processes; prepositioned keying material; DoD-approved or DoD-issued Medium Assurance PKI certificates; DoD-approved or DoD-issued Medium Hardware Assurance PKI certificates and hardware security tokens that	Functional	Equal	Asymmetric Keys	CRY-09.2	Facilitate the production and management of asymmetric cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key management	10		
SC-12(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SC-12(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SC-12(06)	Cryptographic Key Establishment and Management | Physical Control of Keys	Maintain physical control of cryptographic keys when stored information is encrypted by external service providers.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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
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		SC-13
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-13
SC-13(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SC-13(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SC-13(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SC-13(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SC-14		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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	Mechanisms exist to prohibit collaborative computing devices with the following exceptions: (1) Networked whiteboards; (2) Video teleconference	5		SC-15
SC-15(01)	Collaborative Computing Devices and Applications | Physical or Logical Disconnect	Provide [Selection (one or more): physical; logical] disconnect of collaborative computing devices in a manner that supports ease of use.	Functional	Intersects With	Collaborative Computing Devices	END-14	Mechanisms exist to prohibit collaborative computing devices with the following exceptions: (1) Networked whiteboards; (2) Video teleconference	5		
SC-15(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SC-15(03)	Computing Devices and Applications | Disabling and Removal in Secure Work Areas	Disable or remove collaborative computing devices and applications from [Assignment: organization-defined systems or system components] in [Assignment: organization-defined secure work areas].	Functional	Equal	Disabling / Removal In Secure Work Areas	END-14.1	Mechanisms exist to disable or remove collaborative computing devices from critical systems and secure work areas.	10		
SC-15(04)	Collaborative Computing Devices and Applications | Explicitly Indicate Current Participants	Provide an explicit indication of current participants in [Assignment: organization-defined online meetings and teleconferences].	Functional	Equal	Explicitly Indicate Current Participants	END-14.2	Automated mechanisms exist to provide an explicit indication of current participants in online meetings and teleconferences.	10		
SC-16	Transmission of Security and Privacy Attributes	Associate [Assignment: organization-defined security and privacy attributes] with information exchanged between systems and between system components.	Functional	Intersects With	Transmission of Cybersecurity & Data Protection Attributes	CRY-10	Mechanisms exist to associate Technology Assets, Applications and/or Services (TAAS) security attributes with information	5		
SC-16(01)	Transmission of Security and Privacy Attributes | Integrity Verification	Verify the integrity of transmitted security and privacy attributes.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5		
SC-16(01)	Transmission of Security and Privacy Attributes | Integrity Verification	Verify the integrity of transmitted security and privacy attributes.	Functional	Intersects With	Transmission of Cybersecurity & Data Protection Attributes	CRY-10	Mechanisms exist to associate Technology Assets, Applications and/or Services (TAAS) security attributes with information	5		
SC-16(02)	Transmission of Security and Privacy Attributes | Anti-spoofing Mechanisms	Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-16(03)	Transmission of Security and Privacy Attributes | Cryptographic Binding	Implement [Assignment: organization-defined mechanisms or techniques] to bind security and privacy attributes to transmitted information.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-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-18(01)	Mobile Code | Identify Unacceptable Code and Take Corrective Actions	Identify [Assignment: organization-defined unacceptable mobile code] and take [Assignment: organization-defined corrective actions].	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		

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	NIST SP 800-82 Low Overlay
SC-18(01)	Mobile Code | Identify Unacceptable Code and Take Corrective Actions	Identify [Assignment: organization-defined unacceptable mobile code] and take [Assignment: organization-defined corrective actions].	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5		
SC-18(01)	Mobile Code | Identify Unacceptable Code and Take Corrective Actions	Identify [Assignment: organization-defined unacceptable mobile code] and take [Assignment: organization-defined corrective actions].	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5		
SC-18(02)	Mobile Code | Acquisition, Development, and Use	Verify that the acquisition, development, and use of mobile code to be deployed in the system meets [Assignment: organization-defined mobile code requirements].	Functional	Intersects With	Software Licensing Restrictions	AST-02.7	Mechanisms exist to protect Intellectual Property (IP) rights with software licensing restrictions.	5		
SC-18(02)	Mobile Code | Acquisition, Development, and Use	Verify that the acquisition, development, and use of mobile code to be deployed in the system meets [Assignment: organization-defined mobile code requirements].	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5		
SC-18(03)	Mobile Code | Prevent Downloading and Execution	Prevent the download and execution of [Assignment: organization-defined unacceptable mobile code].	Functional	Intersects With	DNS & Content Filtering	NET-18	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-18(03)	Mobile Code | Prevent Downloading and Execution	Prevent the download and execution of [Assignment: organization-defined unacceptable mobile code].	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5		
SC-18(04)	Mobile Code | Prevent Automatic Execution	Prevent the automatic execution of mobile code in [Assignment: organization-defined software applications] and enforce [Assignment: organization-defined actions] prior to executing the code.	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5		
SC-18(04)	Mobile Code | Prevent Automatic Execution	Prevent the automatic execution of mobile code in [Assignment: organization-defined software applications] and enforce [Assignment: organization-defined actions] prior to executing the code.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5		
SC-18(05)	Mobile Code | Allow Execution Only in Confined Environments	Allow execution of permitted mobile code only in confined virtual machine environments.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-19		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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-20
SC-20(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SC-20(02)	Name/address Resolution Service (authoritative Source) | Data	Provide data origin and integrity protection artifacts for internal name/address resolution queries.	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	Secure 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-21
SC-21(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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-22
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-23(01)	Session Authenticity | Invalidate Session Identifiers at Logout	Invalidate session identifiers upon user logout or other session termination.	Functional	Equal	Invalidate Session Identifiers at Logout	NET-09.1	Automated mechanisms exist to invalidate session identifiers upon user logout or other session termination.	10		
SC-23(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SC-23(03)	Session Authenticity | Unique System-generated Session Identifiers	Generate a unique session identifier for each session with [Assignment: organization-defined randomness requirements] and recognize only session identifiers that are system-generated.	Functional	Equal	Unique System-Generated Session Identifiers	NET-09.2	Automated mechanisms exist to generate and recognize unique session identifiers for each session.	10		
SC-23(04)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SC-23(05)	Session Authenticity | Allowed Certificate Authorities	Only allow the use of [Assignment: organization-defined certificate authorities] for verification of the establishment of protected sessions.	Functional	Equal	Certificate Authorities	CRY-11	enable the use of organization-defined Certificate Authorities (CAs) to facilitate the establishment of protected	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-25	Thin Nodes	Employ minimal functionality and information storage on the following system components: [Assignment: organization-defined system components].	Functional	Equal	Thin Nodes	END-11	Mechanisms exist to configure thin nodes to have minimal functionality and information storage.	10		
SC-26	Decoys	Include components within organizational systems specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.	Functional	Equal	Honeypots	SEA-11	honeypots that are specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting and	10		
SC-26(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SC-27	Platform-independent Applications	Include within organizational systems the following platform independent applications: [Assignment: organization-defined platform-independent applications].	Functional	Equal	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	10		
SC-28	Protection of Information at Rest	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5		
SC-28	Protection of Information at Rest	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5		
SC-28(01)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5		
SC-28(01)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5		
SC-28(01)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5		
SC-28(01)	Protection of Information at Rest | Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].	Functional	Intersects With	Encrypting Data In Storage Media	DCH-07.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	5		
SC-28(02)	Protection of Information at Rest | Offline Storage	Remove the following information from online storage and store offline in a secure location: [Assignment: organization-defined information].	Functional	Intersects With	Offline Storage	CRY-05.2	unused data from online storage and archive it off-line in a secure location until it can be disposed of according to data retention	5		
SC-28(02)	Protection of Information at Rest | Offline Storage	Remove the following information from online storage and store offline in a secure location: [Assignment: organization-defined information].	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of	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	NIST SP 800-82 Low Overlay
SC-28(03)	Protection of Information at Rest | Cryptographic Keys	Provide protected storage for cryptographic keys [Selection (one): [Assignment: organization-defined safeguards]; hardware-protected key store].	Functional	Equal	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	10		
SC-29	Heterogeneity	Employ a diverse set of information technologies for the following system components in the implementation of the system: [Assignment: organization-defined system components].	Functional	Equal	Heterogeneity	SEA-13	Mechanisms exist to utilize a diverse set of technologies for system components to reduce the impact of technical vulnerabilities from the same Original Equipment Manufacturer	10		
SC-29(01)	Heterogeneity | Virtualization Techniques	Employ virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [Assignment: organization-defined frequency].	Functional	Equal	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications	10		
SC-30	Concealment and Misdirection	techniques for [Assignment: organization-defined systems] at [Assignment: organization-defined time periods] to confuse and mislead adversaries: [Assignment: organization-defined concealment and	Functional	Intersects With	Concealment & Misdirection	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for Technology Assets, Applications and/or	5		
SC-30(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SC-30(02)	Concealment and Misdirection | Randomness	Employ [Assignment: organization-defined techniques] to introduce randomness into organizational operations and assets.	Functional	Equal	Randomness	SEA-14.1	Automated mechanisms exist to introduce randomness into organizational operations and assets.	10		
SC-30(03)	Concealment and Misdirection | Change Processing and Storage Locations	Change the location of [Assignment: organization-defined processing and/or storage] [Selection (one): [Assignment: organization-defined time frequency]; at random time intervals].	Functional	Equal	Change Processing & Storage Locations	SEA-14.2	Automated mechanisms exist to change the location of processing and/or storage at random time intervals.	10		
SC-30(04)	Concealment and Misdirection | Misleading Information	Employ realistic, but misleading information in [Assignment: organization-defined system components] about its security state or posture.	Functional	Intersects With	Concealment & Misdirection	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for Technology Assets, Applications and/or	5		
SC-30(05)	Concealment and Misdirection | Concealment of System Components	Employ the following techniques to hide or conceal [Assignment: organization-defined system components]: [Assignment: organization-defined techniques].	Functional	Intersects With	Concealment & Misdirection	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for Technology Assets, Applications and/or	5		
SC-31	Covert Channel Analysis	a. Perform a covert channel analysis to identify those aspects of communications within the system that are potential avenues for covert [Selection (one or more): storage; timing] channels; andb. Estimate the maximum bandwidth of these channels.	Functional	Equal	Covert Channel Analysis	MON-15	covert channel analysis to identify aspects of communications that are potential avenues for covert	10		
SC-31(01)	Covert Channel Analysis | Test Covert Channels for Exploitability	Test a subset of the identified covert channels to determine the channels that are exploitable.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-31(02)	Covert Channel Analysis | Maximum Bandwidth	Reduce the maximum bandwidth for identified covert [Selection (one or more): storage; timing] channels to [Assignment: organization-defined values].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-31(03)	Covert Channel Analysis | Measure Bandwidth in Operational Environments	Measure the bandwidth of [Assignment: organization-defined subset of identified covert channels] in the operational environment of the system.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-32	System Partitioning	defined system components] residing in separate [Selection (one): physical; logical] domains or environments based on [Assignment: organization-defined circumstances for physical or logical	Functional	Equal	System Partitioning	SEA-03.1	Mechanisms exist to partition systems so that partitions reside in separate physical domains or environments.	10		
SC-32(01)	System Partitioning | Separate Physical Domains for Privileged Functions	Partition privileged functions into separate physical domains.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-33		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SC-34	Non-modifiable Executable Programs	components], load and execute:a. The operating environment from hardware-enforced, read-only media; andb. The following applications from hardware-enforced, read-only media: [Assignment:	Functional	Equal	Non-Modifiable Executable Programs	SEA-16	modifiable executable programs that load and execute the operating environment and applications from hardware-	10		
SC-34(01)	Non-modifiable Executable Programs | No Writable Storage	Employ [Assignment: organization-defined system components] with no writeable storage that is persistent across component restart or power on/off.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-34(02)	Non-modifiable Executable Programs | Integrity Protection on Read-only Media	Protect the integrity of information prior to storage on read-only media and control the media after such information has been recorded onto the media.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-34(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SC-35	External Malicious Code Identification	Include system components that proactively seek to identify network-based malicious code or malicious websites.	Functional	Equal	Honeyclients	SEA-12	Mechanisms exist to utilize honeyclients that proactively seek to identify malicious websites and/or web-based malicious code.	10		
SC-36	Distributed Processing and Storage	Distribute the following processing and storage components across multiple [Selection (one): physical locations; logical domains]: [Assignment: organization-defined processing and storage components].	Functional	Equal	Distributed Processing & Storage	SEA-15	Mechanisms exist to distribute processing and storage across multiple physical locations.	10		
SC-36(01)	Distributed Processing and Storage | Polling Techniques	faults, errors, or compromises to the following processing and storage components: [Assignment: organization-defined distributed processing and storage components]; andb. Take the following actions in response to identified faults, errors, or compromises:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-36(02)	Distributed Processing and Storage | Synchronization	Synchronize the following duplicate systems or system components: [Assignment: organization-defined duplicate systems or system components].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-37	Out-of-band Channels	physical delivery or electronic transmission of [Assignment: organization-defined information, system components, or devices] to [Assignment: organization-defined individuals or systems]: [Assignment:	Functional	Intersects With	Out-of-Band Channels	NET-11	Mechanisms exist to utilize out-of-band channels for the electronic transmission of information and/or the physical shipment of system components or devices to authorized	5		
SC-37(01)	Out-of-band Channels | Ensure Delivery and Transmission	ensure that only [Assignment: organization-defined individuals or systems] receive the following information, system components, or devices: [Assignment: organization-defined information, system	Functional	Intersects With	Out-of-Band Channels	NET-11	Mechanisms exist to ensure that only authorized recipients receive the electronic transmission of information and/or the physical shipment of system components	5		
SC-38	Operations Security	Employ the following operations security controls to protect key organizational information throughout the system development life cycle: [Assignment: organization-defined operations security controls].	Functional	Intersects With	Security Operations Center (SOC)	OPS-04	Mechanisms exist to establish and maintain a Security Operations Center (SOC) that facilitates a 24x7 response capability.	5		
SC-38	Operations Security	Employ the following operations security controls to protect key organizational information throughout the system development life cycle: [Assignment: organization-defined operations security controls].	Functional	Intersects With	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	5		
SC-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-39
SC-39(01)	Process Isolation | Hardware Separation	Implement hardware separation mechanisms to facilitate process isolation.	Functional	Equal	Hardware Separation	SEA-04.2	Mechanisms exist to implement underlying hardware separation mechanisms to facilitate process separation.	10		
SC-39(02)	Process Isolation | Separate Execution Domain Per Thread	Maintain a separate execution domain for each thread in [Assignment: organization-defined multi-threaded processing].	Functional	Equal	Thread Separation	SEA-04.3	Mechanisms exist to maintain a separate execution domain for each thread in multi-threaded processing.	10		
SC-40	Wireless Link Protection	Protect external and internal [Assignment: organization-defined wireless links] from the following signal parameter attacks: [Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks].	Functional	Intersects With	Wireless Link Protection	NET-12.1	attacks through monitoring for unauthorized wireless connections, including scanning for unauthorized wireless access	5		
SC-40	Wireless Link Protection	Protect external and internal [Assignment: organization-defined wireless links] from the following signal parameter attacks: [Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks].	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication	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	NIST SP 800-82 Low Overlay
SC-40(01)	Wireless Link Protection | Electromagnetic Interference	Implement cryptographic mechanisms that achieve [Assignment: organization-defined level of protection] against the effects of intentional electromagnetic interference.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-40(02)	Wireless Link Protection | Reduce Detection Potential	Implement cryptographic mechanisms to reduce the detection potential of wireless links to [Assignment: organization-defined level of reduction].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-40(03)	Protection | Imitative or Manipulative Communications	Implement cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-40(04)	Wireless Link Protection | Signal Parameter Identification	Implement cryptographic mechanisms to prevent the identification of [Assignment: organization-defined wireless transmitters] by using the transmitter signal parameters.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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-41
SC-42	Sensor Capability and Data	[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	Sensor Capability	END-13	Embedded sensors on systems to: (1) Prohibit the remote activation of sensing capabilities; and (2) Provide an explicit indication	10		
SC-42(01)	Sensor Capability and Data | Reporting to Authorized Individuals or Roles	Verify that the system is configured so that data or information collected by the [Assignment: organization-defined sensors] is only reported to authorized individuals or roles.	Functional	Equal	Sensor Delivery Verification	END-13.4	embedded technology sensors are configured so that data collected by the sensor(s) is only reported to authorized	10		
SC-42(02)	Sensor Capability and Data | Authorized Use	Employ the following measures so that data or information collected by [Assignment: organization-defined sensors] is only used for authorized purposes: [Assignment: organization-defined measures].	Functional	Equal	Authorized Use	END-13.1	Mechanisms exist to utilize organization-defined measures so that data or information collected by sensors is only used for authorized purposes.	10		
SC-42(03)	Withdrawn		Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SC-42(04)	Sensor Capability and Data | Notice of Collection	Employ the following measures to facilitate an individual's awareness that personally identifiable information is being collected by [Assignment: organization-defined sensors]: [Assignment: organization-defined measures].	Functional	Equal	Notice of Collection	END-13.2	Mechanisms exist to notify individuals that Personal Data (PD) is collected by sensors.	10		
SC-42(05)	Sensor Capability and Data | Collection Minimization	Employ [Assignment: organization-defined sensors] that are configured to minimize the collection of information about individuals that is not needed.	Functional	Equal	Collection Minimization	END-13.3	Mechanisms exist to utilize sensors that are configured to minimize the collection of information about individuals.	10		
SC-43	Usage Restrictions	a. Establish usage restrictions and implementation guidelines for the following system components: [Assignment: organization-defined system components]; andb. Authorize, monitor, and control the use of such components within the system.	Functional	Equal	Usage Parameters	AST-14	enforce usage parameters that limit the potential damage caused from the unauthorized or unintentional alteration of	10		
SC-44	Detonation Chambers	Employ a detonation chamber capability within [Assignment: organization-defined system, system component, or location].	Functional	Equal	Detonation Chambers (Sandboxes)	IRO-15	Mechanisms exist to utilize a detonation chamber capability to detect and/or block potentially-malicious files and email attachments.	10		
SC-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-45
SC-45(01)	System Time Synchronization | Synchronization with Authoritative Time Source	[Selection (one): organization-defined time period; organization-defined frequency] with [Assignment: organization-defined authoritative time source]; andb. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time	Functional	Equal	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	10		
SC-45(02)	System Time Synchronization | Secondary Authoritative Time Source	is in a different geographic region than the primary authoritative time source; andb. Synchronize the internal system clocks to the secondary authoritative time source if the primary authoritative time source is	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-46	Cross Domain Policy Enforcement	Implement a policy enforcement mechanism [Selection (one): physically; logically] between the physical and/or network interfaces for the connecting security domains.	Functional	Equal	Cross Domain Solution (CDS)	NET-02.3	Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security	10		
SC-47	Alternate Communications Channels	Establish [Assignment: organization-defined alternate communications paths] for system operations organizational command and control.	Functional	Equal	Alternate Communications Channels	BCD-10.4	command and control capabilities via alternate communications channels and designating alternative decision makers if primary decision	10		
SC-48	Sensor Relocation	Relocate [Assignment: organization-defined sensors and monitoring capabilities] to [Assignment: organization-defined locations] under the following conditions or circumstances: [Assignment: organization-defined conditions or circumstances].	Functional	Intersects With	Threat Hunting	THR-07	cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security	5		
SC-48	Sensor Relocation	Relocate [Assignment: organization-defined sensors and monitoring capabilities] to [Assignment: organization-defined locations] under the following conditions or circumstances: [Assignment: organization-defined conditions or circumstances].	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation	5		
SC-48(01)	Sensor Relocation | Dynamic Relocation of Sensors or Monitoring Capabilities	Dynamically relocate [Assignment: organization-defined sensors and monitoring capabilities] to [Assignment: organization-defined locations] under the following conditions or circumstances: [Assignment: organization-defined conditions or circumstances].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-49	Hardware-enforced Separation and Policy Enforcement	Implement hardware-enforced separation and policy enforcement mechanisms between [Assignment: organization-defined security domains].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-50	Software-enforced Separation and Policy Enforcement	Implement software-enforced separation and policy enforcement mechanisms between [Assignment: organization-defined security domains].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SC-51	Hardware-based Protection	[Assignment: organization-defined system firmware components]; andb. Implement specific procedures for [Assignment: organization-defined authorized individuals] to manually disable hardware write-protect for firmware modifications and re-enable the write-	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-01	Policy and Procedures	regulations, policies, standards, and guidelines; andz. 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
SI-01	Policy and Procedures	regulations, policies, standards, and guidelines; andz. 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
SI-01	Policy and Procedures	regulations, policies, standards, and guidelines; andz. 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-01
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
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
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
SI-02(01)	Withdrawn		Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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		

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	NIST SP 800-82 Low Overlay
SI-02(03)	Flaw Remediation | Time to Remediate Flaws and Benchmarks for Corrective Actions	a. Measure the time between flaw identification and flaw remediation; andb. Establish the following benchmarks for taking corrective actions: [Assignment: organization-defined benchmarks].	Functional	Equal	Time To Remediate / Benchmarks For Corrective Action	VPM-05.3	Mechanisms exist to track the effectiveness of remediation operations through metrics reporting.	10		
SI-02(04)	Flaw Remediation | Automated Patch Management Tools	Employ automated patch management tools to facilitate flaw remediation to the following system components: [Assignment: organization-defined system components].	Functional	Intersects With	Automated Remediation Status	VPM-05.2	Automated mechanisms exist to determine the state of system components with regard to flaw remediation.	5		
SI-02(04)	Flaw Remediation | Automated Patch Management Tools	Employ automated patch management tools to facilitate flaw remediation to the following system components: [Assignment: organization-defined system components].	Functional	Intersects With	Automated Software & Firmware Updates	VPM-05.4	Automated mechanisms exist to install the latest stable versions of security-relevant software and firmware updates.	5		
SI-02(04)	Flaw Remediation | Automated Patch Management Tools	Employ automated patch management tools to facilitate flaw remediation to the following system components: [Assignment: organization-defined system components].	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5		
SI-02(04)	Flaw Remediation | Automated Patch Management Tools	Employ automated patch management tools to facilitate flaw remediation to the following system components: [Assignment: organization-defined system components].	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services	5		
SI-02(05)	Flaw Remediation | Automatic Software and Firmware Updates	Install [Assignment: organization-defined security-relevant software and firmware updates] automatically to [Assignment: organization-defined system components].	Functional	Intersects With	Automated Software & Firmware Updates	VPM-05.4	Automated mechanisms exist to install the latest stable versions of security-relevant software and firmware updates.	5		
SI-02(06)	Flaw Remediation | Removal of Previous Versions of Software and Firmware	Remove previous versions of [Assignment: organization-defined software and firmware components] after updated versions have been installed.	Functional	Equal	Removal of Previous Versions	VPM-05.5	Mechanisms exist to remove old versions of software and firmware components after updated versions have been installed.	10		
SI-02(07)	Flaw Remediation | Root Cause Analysis	underlying causes of issues or failures; b. Develop actions to address the root cause of the issue or failure; c. Implement the actions and monitor the	Functional	Equal	Software Design Root Cause Analysis	TDA-06.6	Mechanisms exist to assess software design processes that includes: (1) Conducting Root Cause	10		
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
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
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		SI-03
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
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	Mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public	5		SI-03
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
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-03
SI-03(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SI-03(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SI-03(03)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SI-03(04)	Malicious Code Protection | Updates Only by Privileged Users	Update malicious code protection mechanisms only when directed by a privileged user.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-03(05)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SI-03(06)	Malicious Code Protection | Testing and Verification	a. Test malicious code protection mechanisms [Assignment: organization-defined frequency] by introducing known benign code into the system; andb. Verify that the detection of the code and the associated incident reporting occur	Functional	Equal	Malware Protection Mechanism Testing	END-04.5	introducing a known benign, non-spreading test case into the system and subsequently verifying that both detection of	10		
SI-03(07)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SI-03(08)	Malicious Code Protection | Detect Unauthorized Commands	programming interface on [Assignment: organization-defined system hardware components]: [Assignment: organization-defined unauthorized operating system commands]; andb. [Selection (one or more): issue a	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-03(09)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SI-03(10)	Malicious Code Protection | Malicious Code Analysis	analyze the characteristics and behavior of malicious code: [Assignment: organization-defined tools and techniques]; andb. Incorporate the results from malicious code analysis into organizational incident	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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
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
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
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
SI-04(01)	System Monitoring | System-wide Intrusion Detection System	Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.	Functional	Equal	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke	10		
SI-04(02)	System Monitoring | Automated Tools and Mechanisms for Real-time Analysis	Employ automated tools and mechanisms to support near real-time analysis of events.	Functional	Equal	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation	10		
SI-04(03)	System Monitoring | Automated Tool and Mechanism Integration	Employ automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access control and flow control mechanisms.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-04(04)	System Monitoring | Inbound and Outbound Communications Traffic	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 activities	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	alert [Assignment: organization-defined personnel or 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(06)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SI-04(07)	System Monitoring | Automated Response to Suspicious Events	response personnel (identified by name and/or by role)] of detected suspicious events; andb. Take the following actions upon detection: [Assignment: organization-defined least-disruptive actions to	Functional	Intersects With	Automated Response to Suspicious Events	MON-01.11	Automated mechanisms exist to implement pre-determined corrective actions in response to detected events that have	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	NIST SP 800-82 Low Overlay
SI-04(07)	System Monitoring | Automated Response to Suspicious Events	response personnel (identified by name and/or by role)] of detected suspicious events; andb. Take the following actions upon detection: [Assignment: organization-defined least-disruptive actions to	Functional	Intersects With	Automated Incident Handling Processes	IRO-02.1	Automated mechanisms exist to support the incident handling process.	5		
SI-04(08)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SI-04(09)	System Monitoring | Testing of Monitoring Tools and Mechanisms	Test intrusion-monitoring tools and mechanisms [Assignment: organization-defined frequency].	Functional	Intersects With	Incident Response Testing	IRO-06	incident response capabilities through realistic exercises to determine the operational effectiveness of those	5		
SI-04(10)	System Monitoring | Visibility of Encrypted Communications	Make provisions so that [Assignment: organization-defined encrypted communications traffic] is visible to [Assignment: organization-defined system monitoring tools and mechanisms].	Functional	Equal	Visibility of Encrypted Communications	NET-18.2	Mechanisms exist to configure the proxy to make encrypted communications traffic visible to monitoring tools and mechanisms.	10		
SI-04(11)	System Monitoring | Analyze Communications Traffic Anomalies	Analyze outbound communications traffic at the external interfaces to the system and selected [Assignment: organization-defined interior points within the system] to discover anomalies.	Functional	Equal	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to	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(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	Real-Time Alerts of Event Logging Failure	MON-05.1	Mechanisms exist to provide 24x7x365 near real-time alerting capability when an event log processing failure occurs.	5		
SI-04(13)	System Monitoring | Analyze Traffic and Event Patterns	a. Analyze communications traffic and event patterns for the system;b. Develop profiles representing common traffic and event patterns; andc. Use the traffic and event profiles in tuning system-monitoring devices	Functional	Equal	Alert Threshold Tuning	MON-01.13	monitoring technologies through analyzing communications traffic/event patterns and developing profiles representing common traffic patterns and/or	10		
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(15)	System Monitoring | Wireless to Wireline Communications	Employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.	Functional	Intersects With	Wireless Intrusion Detection / Prevention Systems (WIDS / WIPS) Deployment	NET-08.2	Mechanisms exist to utilize Wireless Intrusion Detection / Protection Systems (WIDS / WIPS) on wireless network segments	5		
SI-04(16)	System Monitoring | Correlate Monitoring Information	Correlate information from monitoring tools and mechanisms employed throughout the system.	Functional	Equal	Correlate Monitoring Information	MON-02.1	technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to	10		
SI-04(17)	System Monitoring | Integrated Situational Awareness	Correlate information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.	Functional	Equal	Integration of Scanning & Other Monitoring Information	MON-02.3	records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further	10		
SI-04(18)	System Monitoring | Analyze Traffic and Covert Exfiltration	Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information: [Assignment: organization-defined interior points within the system]	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5		
SI-04(18)	System Monitoring | Analyze Traffic and Covert Exfiltration	Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information: [Assignment: organization-defined interior points within the system]	Functional	Intersects With	Analyze Traffic for Covert Exfiltration	MON-11.1	Automated mechanisms exist to analyze network traffic to detect covert data exfiltration.	5		
SI-04(19)	System Monitoring | Risk for Individuals	Implement [Assignment: organization-defined additional monitoring] of individuals who have been identified by [Assignment: organization-defined sources] as posing an increased level of risk.	Functional	Equal	Individuals Posing Greater Risk	MON-01.14	Mechanisms exist to implement enhanced activity monitoring for individuals who have been identified as posing an increased level of risk.	10		
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(21)	System Monitoring | Probationary Periods	Implement the following additional monitoring of individuals during [Assignment: organization-defined probationary period]: [Assignment: organization-defined additional monitoring].	Functional	Equal	Probationary Periods	HRS-02.2	Mechanisms exist to identify newly onboarded personnel for enhanced monitoring during their probationary period.	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-04(23)	System Monitoring | Host-based Devices	Implement the following host-based monitoring mechanisms at [Assignment: organization-defined system components]: [Assignment: organization-defined host-based monitoring mechanisms].	Functional	Equal	Host-Based Devices	MON-01.6	Prevention Systems (HIDS / HIPS) to actively alert on or block unwanted activities and send logs to a Security Incident Event Manager (SIEM), or similar	10		
SI-04(24)	System Monitoring | Indicators of Compromise	Discover, collect, and distribute to [Assignment: organization-defined personnel or roles], indicators of compromise provided by [Assignment: organization-defined sources].	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	5		
SI-04(24)	System Monitoring | Indicators of Compromise	Discover, collect, and distribute to [Assignment: organization-defined personnel or roles], indicators of compromise provided by [Assignment: organization-defined sources].	Functional	Intersects With	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets,	5		
SI-04(25)	System Monitoring | Optimize Network Traffic Analysis	Provide visibility into network traffic at external and key internal system interfaces to optimize the effectiveness of monitoring devices.	Functional	Intersects With	Limit Network Connections	NET-03.1	Mechanisms exist to limit the number of concurrent external network connections to its Technology Assets, Applications	5		
SI-04(25)	System Monitoring | Optimize Network Traffic Analysis	Provide visibility into network traffic at external and key internal system interfaces to optimize the effectiveness of monitoring devices.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke	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	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5		SI-05
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
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-05
SI-05(01)	Security Alerts, Advisories, and Directives | Automated Alerts and Advisories	Broadcast security alert and advisory information throughout the organization using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Threat Intelligence Feeds	THR-03	vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of	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-06(01)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SI-06(02)	Privacy Function Verification | Automation Support for Distributed	Implement automated mechanisms to support the management of distributed security and privacy function testing.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-06(03)	Security and Privacy Function Verification | Report Verification Results	Report the results of security and privacy function verification to [Assignment: organization-defined personnel or roles].	Functional	Equal	Report Verification Results	CHG-06.1	Mechanisms exist to report the results of security, compliance and resilience capability verification to appropriate organizational management	10		
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		

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	NIST SP 800-82 Low Overlay
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(03)	Software, Firmware, and Information Integrity | Centrally Managed Integrity Tools	Employ centrally managed integrity verification tools.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-07(04)	Withdrawn		Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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(06)	Software, Firmware, and Information Integrity | Cryptographic Protection	Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.	Functional	Equal	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10		
SI-07(07)	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(08)	Software, Firmware, and Information Integrity | Auditing Capability for Significant Events	provide the capability to audit the event and initiate the following actions: [Selection (one or more): generate an audit record; alert current user; alert [Assignment: organization-defined personnel or roles];	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-07(09)	Software, Firmware, and Information Integrity | Verify Boot Process	Verify the integrity of the boot process of the following system components: [Assignment: organization-defined system components].	Functional	Equal	Boot Process Integrity	END-06.5	Automated mechanisms exist to verify the integrity of the boot process of systems.	10		
SI-07(10)	Software, Firmware, and Information Integrity | Protection of Boot Firmware	Implement the following mechanisms to protect the integrity of boot firmware in [Assignment: organization-defined system components]: [Assignment: organization-defined mechanisms].	Functional	Equal	Protection of Boot Firmware	END-06.6	Automated mechanisms exist to protect the integrity of boot firmware in systems.	10		
SI-07(11)	Withdrawn		Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SI-07(12)	Software, Firmware, and Information Integrity | Integrity Verification	Require that the integrity of the following user-installed software be verified prior to execution: [Assignment: organization-defined user-installed software].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-07(13)	Withdrawn		Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SI-07(14)	Withdrawn		Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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 an organization-approved	5		
SI-07(16)	and Information Integrity | Time Limit on Process Execution Without	Prohibit processes from executing without supervision for more than [Assignment: organization-defined time period].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-07(17)	Software, Firmware, and Information Integrity | Runtime Application Self-protection	Implement [Assignment: organization-defined controls] for application self-protection at runtime.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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		
SI-08(01)	Withdrawn		Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SI-08(02)	Spam Protection | Automatic Updates	Automatically update spam protection mechanisms [Assignment: organization-defined frequency].	Functional	Equal	Automatic Spam and Phishing Protection Updates	END-08.2	automatically update anti-phishing and spam protection technologies when new releases are available in accordance with configuration and change	10		
SI-08(03)	Spam Protection | Continuous Learning Capability	Implement spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-09	Withdrawn		Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
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-10(01)	Information Input Validation | Manual Override Capability	validation of the following information inputs: [Assignment: organization-defined inputs defined in the base control (SI-10)];b. Restrict the use of the manual override capability to only [Assignment: organization-defined authorized individuals]; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-10(02)	Information Input Validation | Review and Resolve Errors	Review and resolve input validation errors within [Assignment: organization-defined time period].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-10(03)	Information Input Validation | Predictable Behavior	Verify that the system behaves in a predictable and documented manner when invalid inputs are received.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-10(04)	Information Input Validation | Timing Interactions	Account for timing interactions among system components in determining appropriate responses for invalid inputs.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-10(05)	Information Input Validation | Restrict Inputs to Trusted Sources and Approved Formats	Restrict the use of information inputs to [Assignment: organization-defined trusted sources] and/or [Assignment: organization-defined formats].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-10(06)	Information Input Validation | Injection Prevention	Prevent untrusted data injections.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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-12

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	NIST SP 800-82 Low Overlay
SI-12(01)	Management and Retention | Limit Personally Identifiable Information	Limit personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: [Assignment: organization-defined elements of personally identifiable information]	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that:	5		
SI-12(01)	Management and Retention | Limit Personally Identifiable Information	Limit personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: [Assignment: organization-defined elements of personally identifiable information]	Functional	Intersects With	Minimize Sensitive / Regulated Data	DCH-18.1	Mechanisms exist to minimize sensitive/regulated data that is collected, received, processed, stored and/or transmitted	5		
SI-12(02)	Retention | Minimize Personally Identifiable Information in	Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: [Assignment: organization-defined techniques].	Functional	Intersects With	Limit Sensitive / Regulated Data In Testing, Training & Research	DCH-18.2	the use of sensitive/regulated data for research, testing, or training, in accordance with authorized, legitimate business	5		
SI-12(02)	Retention | Minimize Personally Identifiable Information in	Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: [Assignment: organization-defined techniques].	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that:	5		
SI-12(03)	Management and Retention | Information Disposal	Use the following techniques to dispose of, destroy, or erase information following the retention period: [Assignment: organization-defined techniques].	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period	5		
SI-12(03)	Management and Retention | Information Disposal	Use the following techniques to dispose of, destroy, or erase information following the retention period: [Assignment: organization-defined techniques].	Functional	Intersects With	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	5		
SI-13	Predictable Failure Prevention	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-13(01)	Predictable Failure Prevention | Transferring Component Responsibilities	Take system components out of service by transferring component responsibilities to substitute components no later than [Assignment: organization-defined fraction or percentage] of mean time to failure.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-13(02)		Withdrawn	Functional	No Relationship	N/A	N/A	N/A	0		Withdrawn
SI-13(03)	Predictable Failure Prevention | Manual Transfer Between Components	Manually initiate transfers between active and standby system components when the use of the active component reaches [Assignment: organization-defined percentage] of the mean time to failure.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-13(04)	Prevention | Standby Component Installation and	that the standby components are successfully and transparently installed within [Assignment: organization-defined time period]; andb. [Selection (one or more): Activate [Assignment: organization-defined alarm]; Automatically shut down the system;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-13(05)	Predictable Failure Prevention | Failover Capability	Provide [Selection (one): real-time; near real-time] [Assignment: organization-defined failover capability] for the system.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-14	Non-persistence	Implement non-persistent [Assignment: organization-defined system components and services] that are initiated in a known state and terminated [Selection (one or more): upon end of session of use; periodically at [Assignment: organization-defined frequency]]	Functional	Equal	Non-Persistence	SEA-08	components and services that are initiated in a known state and terminated upon the end of the session of use or periodically at	10		
SI-14(01)	Non-persistence | Refresh from Trusted Sources	Obtain software and data employed during system component and service refreshes from the following trusted sources: [Assignment: organization-defined trusted sources].	Functional	Equal	Refresh from Trusted Sources	SEA-08.1	Mechanisms exist to ensure that software and data needed for system component and service refreshes are obtained from	10		
SI-14(02)	Non-persistence | Non-persistent Information	a. [Selection (one): Refresh [Assignment: organization-defined information] [Assignment: organization-defined frequency]; Generate [Assignment: organization-defined information] on demand]; andb. Delete information when no longer needed.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-14(03)	Non-persistence | Non-persistent Connectivity	Establish connections to the system on demand and terminate connections after [Selection (one): completion of a request; a period of non-use].	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-15	Information Output Filtering	Validate information output from the following software programs and/or applications to ensure that the information is consistent with the expected content: [Assignment: organization-defined software programs and/or applications]	Functional	Equal	Information Output Filtering	SEA-09	information output from software programs and/or applications to ensure that the information is consistent with the expected	10		
SI-16	Memory Protection	Implement the following controls to protect the system memory from unauthorized code execution: [Assignment: organization-defined controls].	Functional	Equal	Memory Protection	SEA-10	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	10		
SI-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		SI-17
SI-18	Personally Identifiable Information Quality Operations	completeness of personally identifiable information across the information life cycle [Assignment: organization-defined frequency]; andb. Correct or delete inaccurate or outdated 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		
SI-18(01)	Personally Identifiable Information Quality Operations | Automation Support	Correct or delete personally identifiable information that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified using [Assignment: organization-defined automated mechanisms]	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		
SI-18(02)	Personally Identifiable Information Quality Operations | Data Tags	Employ data tags to automate the correction or deletion of personally identifiable information across the information life cycle within organizational systems.	Functional	Equal	Data Tags	DCH-22.2	Mechanisms exist to utilize data tags to automate tracking of sensitive/regulated data across the information lifecycle.	10		
SI-18(03)	Personally Identifiable Information Quality Operations | Collecting	Collect personally identifiable information directly from the individual.	Functional	Equal	Primary Source Personal Data (PD) Collection	DCH-22.3	Mechanisms exist to collect Personal Data (PD) directly from the individual.	10		
SI-18(04)	Personally Identifiable Information Quality Operations | Individual Requests	Correct or delete personally identifiable information upon request by individuals or their designated representatives.	Functional	Intersects With	Correcting Inaccurate Personal Data (PD)	PRI-06.1	(1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and (2) Disseminating corrections or	5		
SI-18(04)	Personally Identifiable Information Quality Operations | Individual Requests	Correct or delete personally identifiable information upon request by individuals or their designated representatives.	Functional	Intersects With	Updating & Correcting Personal Data (PD)	DCH-22.1	technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-	5		
SI-18(04)	Personally Identifiable Information Quality Operations | Individual Requests	Correct or delete personally identifiable information upon request by individuals or their designated representatives.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data	5		
SI-18(05)	Identifiable Information Quality Operations | Notice of Correction or	Notify [Assignment: organization-defined recipients of personally identifiable information] and individuals that the personally identifiable information has been corrected or deleted.	Functional	Intersects With	Updating & Correcting Personal Data (PD)	DCH-22.1	technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-	5		
SI-18(05)	Identifiable Information Quality Operations | Notice of Correction or	Notify [Assignment: organization-defined recipients of personally identifiable information] and individuals that the personally identifiable information has been corrected or deleted.	Functional	Intersects With	Correcting Inaccurate Personal Data (PD)	PRI-06.1	(1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and (2) Disseminating corrections or	5		
SI-18(05)	Identifiable Information Quality Operations | Notice of Correction or	Notify [Assignment: organization-defined recipients of personally identifiable information] and individuals that the personally identifiable information has been corrected or deleted.	Functional	Intersects With	Notice of Correction or Processing Change	PRI-06.2	Mechanisms exist to notify affected data subjects if their Personal Data (PD) has been corrected, amended or deleted.	5		
SI-19	De-identification	identifiable information from datasets: [Assignment: organization-defined elements of personally identifiable information]; andb. Evaluate [Assignment: organization-defined frequency] for effectiveness of	Functional	Equal	De-Identification (Anonymization)	DCH-23	Mechanisms exist to anonymize data by removing Personal Data (PD) from datasets.	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	NIST SP 800-82 Low Overlay
SI-19(01)	De-identification | Collection	De-identify the dataset upon collection by not collecting personally identifiable information.	Functional	Intersects With	Primary Source Personal Data (PD) Collection	DCH-22.3	Mechanisms exist to collect Personal Data (PD) directly from the individual.	5		
SI-19(01)	De-identification | Collection	De-identify the dataset upon collection by not collecting personally identifiable information.	Functional	Intersects With	De-Identify Dataset Upon Collection	DCH-23.1	Mechanisms exist to de-identify the dataset upon collection by not collecting Personal Data (PD).	5		
SI-19(02)	De-identification | Archiving	Prohibit archiving of personally identifiable information elements if those elements in a dataset will not be needed after the dataset is archived.	Functional	Equal	Archiving	DCH-23.2	Mechanisms exist to refrain from archiving Personal Data (PD) elements if those elements in a dataset will not be needed after the dataset is archived.	10		
SI-19(03)	De-identification | Release	Remove personally identifiable information elements from a dataset prior to its release if those elements in the dataset do not need to be part of the data release.	Functional	Equal	Release	DCH-23.3	Personal Data (PD) elements from a dataset prior to its release if those elements in the dataset do not need to be part of the	10		
SI-19(04)	Removal, Masking, Encryption, Hashing, or Replacement of	Remove, mask, encrypt, hash, or replace direct identifiers in a dataset.	Functional	Intersects With	Data Masking	PRI-05.3	Mechanisms exist to mask sensitive/regulated data through data anonymization, pseudonymization, redaction or de-identification	5		
SI-19(04)	Removal, Masking, Encryption, Hashing, or Replacement of	Remove, mask, encrypt, hash, or replace direct identifiers in a dataset.	Functional	Intersects With	Removal, Masking, Encryption, Hashing or Replacement of Direct Identifiers	DCH-23.4	Mechanisms exist to remove, mask, encrypt, hash or replace direct identifiers in a dataset.	5		
SI-19(05)	De-identification | Statistical Disclosure Control	Manipulate numerical data, contingency tables, and statistical findings so that no individual or organization is identifiable in the results of the analysis.	Functional	Equal	Statistical Disclosure Control	DCH-23.5	numerical data, contingency tables and statistical findings so that no person or organization is identifiable in the results of the	10		
SI-19(06)	De-identification | Differential Privacy	Prevent disclosure of personally identifiable information by adding non-deterministic noise to the results of mathematical operations before the results are reported.	Functional	Equal	Differential Data Privacy	DCH-23.6	disclosure of Personal Data (PD) by adding non-deterministic noise to the results of mathematical operations before	10		
SI-19(07)	De-identification | Validated Algorithms and Software	Perform de-identification using validated algorithms and software that is validated to implement the algorithms.	Functional	Equal	Automated De-Identification of Sensitive Data	DCH-23.7	identification of sensitive/regulated data, using validated algorithms and software to implement the	10		
SI-19(08)	De-identification | Motivated Intruder	Perform a motivated intruder test on the de-identified dataset to determine if the identified data remains or if the de-identified data can be re-identified.	Functional	Equal	Motivated Intruder	DCH-23.8	motivated intruder test on the de-identified dataset to determine if the identified data remains or if the de-identified	10		
SI-20	Tainting	Embed data or capabilities in the following systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization: [Assignment: organization-defined systems or system components].	Functional	Equal	Tainting	THR-08	data or steganographic data in files to enable the organization to determine if data has been exfiltrated and provide a means to identify the individual(s)	10		
SI-21	Information Refresh	Refresh [Assignment: organization-defined information] at [Assignment: organization-defined frequencies] or generate the information on demand and delete the information when no longer needed.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-22	Information Diversity	essential functions and services]; [Assignment: organization-defined alternative information sources]; andb. Use an alternative information source for the execution of essential functions or services on [Assignment: organization-defined systems or system	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SI-23	Information Fragmentation	[Assignment: organization-defined information]; andb. Distribute the fragmented information across the following systems or system components: [Assignment: organization-defined systems or system	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
SR-01	Policy and Procedures	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
SR-01	Policy and Procedures	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
SR-01	Policy and Procedures	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-01
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	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
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
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-02(01)
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-03
SR-03(01)	Supply Chain Controls and Processes | Diverse Supply Base	Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].	Functional	Intersects With	Development Methods, Techniques & Processes	TDA-02.3	processes employ industry-recognized secure practices for secure programming, engineering methods, quality	5		
SR-03(01)	Supply Chain Controls and Processes | Diverse Supply Base	Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].	Functional	Intersects With	Supply Chain Diversity	TDA-03.1	Mechanisms exist to obtain security, compliance and resilience technologies from different suppliers to minimize supply chain risk	5		
SR-03(01)	Supply Chain Controls and Processes | Diverse Supply Base	Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of	5		
SR-03(02)	Supply Chain Controls and Processes | Limitation of Harm	Employ the following controls to limit harm from potential adversaries identifying and targeting the organizational supply chain: [Assignment: organization-defined controls].	Functional	Equal	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain	10		
SR-03(03)	Supply Chain Controls and Processes | Sub-tier Flow Down	Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with	5		
SR-03(03)	Supply Chain Controls and Processes | Sub-tier Flow Down	Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-	5		
SR-04	Provenance	Document, monitor, and maintain valid provenance of the following systems, system components, and associated data: [Assignment: organization-defined systems, system components, and associated data].	Functional	Intersects With	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to Technology Assets, Applications,	5		
SR-04(01)	Provenance | Identity	following supply chain elements, processes, and personnel associated with the identified system and critical system components: [Assignment: organization-defined supply chain elements,	Functional	Intersects With	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to Technology Assets, Applications,	5		
SR-04(02)	Provenance | Track and Trace	establish and maintain unique identification of the following systems and critical system components for tracking through the supply chain: [Assignment: organization-defined systems and critical system components].	Functional	Intersects With	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to Technology Assets, Applications,	5		
SR-04(03)	Provenance | Validate as Genuine and Not Altered	Employ the following controls to validate that the system or system component received is genuine and has not been altered: [Assignment: organization-defined controls].	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means	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	NIST SP 800-82 Low Overlay
SR-04(04)	Provenance | Supply Chain Integrity — Pedigree	and conduct [Assignment: organization-defined analysis] to ensure the integrity of the system and system components by validating the internal composition and provenance of critical or mission-	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-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
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-05(02)	and Methods | Assessments Prior to Selection, Acceptance,	Assess the system, system component, or system service prior to selection, acceptance, modification, or update.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control	
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 security, compliance and	5		
SR-06(01)	Supplier Assessments and Reviews | Testing and Analysis	analysis, independent third-party analysis, organizational testing; independent third-party testing] of the following supply chain elements, processes, and actors associated with the system, system component, or system service: [Assignment: organization-defined	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 security, compliance and	5		
SR-07	Supply Chain Operations Security	Employ the following Operations Security (OPSEC) controls to protect supply chain-related information for the system, system component, or system service: [Assignment: organization-defined Operations Security (OPSEC) controls]	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development,	5		
SR-07	Supply Chain Operations Security	Employ the following Operations Security (OPSEC) controls to protect supply chain-related information for the system, system component, or system service: [Assignment: organization-defined Operations Security (OPSEC) controls]	Functional	Intersects With	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	5		
SR-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-08
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
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-10
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
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(01)
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-11(02)
SR-11(03)	Component Authenticity | Anti-counterfeit Scanning	Scan for counterfeit system components [Assignment: organization-defined frequency].	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-11	authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means	5		
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		SR-12