NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document : Secure Controls Framework (SCF) version 2025.4
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: GovRAMP (based on existing 2022 StateRAMP mappings)
Focal Document URL: https://govramp.org/documents/
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-general-govramp.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
AC-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 manage the development, documentation, and dissemination of the access control policy and procedures; andc. Review and update the current access control:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5			AC-01	AC-01	AC-01	AC-01
AC-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 manage the development, documentation, and dissemination of the access control policy and procedures; andc. Review and update the current access control:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5			AC-01	AC-01	AC-01	AC-01
AC-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 manage the development, documentation, and dissemination of the access control policy and procedures; andc. Review and update the current access control:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-	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-01	AC-01	AC-01
AC-02	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system;b. Assign account managers;c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;d. Specify:1. Authorized users of the system;2. Group and role membership; and3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];g. Monitor the 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 users are terminated or transferred; and3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual;i. Authorize access to the system based on:1. A valid access authorization;2. Intended system usage; and3. [Assignment: organization-defined attributes (as required)];j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; andl. Align account management processes with personnel termination and transfer processes.	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	AC-02	AC-02	AC-02
AC-02	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system;b. Assign account managers;c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;d. Specify:1. Authorized users of the system;2. Group and role membership; and3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];g. Monitor the 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 users are terminated or transferred; and3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual;i. Authorize access to the system based on:1. A valid access authorization;2. Intended system usage; and3. [Assignment: organization-defined attributes (as required)];j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; andl. Align account management processes with personnel termination and transfer processes.	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	AC-02	AC-02	AC-02

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
AC-02	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system;b. Assign account managers;c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;d. Specify:1. Authorized users of the system;2. Group and role membership; and3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];g. Monitor the 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 users are terminated or transferred; and3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual;i. Authorize access to the system based on:1. A valid access authorization;2. Intended system usage; and3. [Assignment: organization-defined attributes (as required)];j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; andl. Align account management processes with personnel termination and transfer processes.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5		AC-02	AC-02	AC-02	AC-02	AC-02
AC-02	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system;b. Assign account managers;c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;d. Specify:1. Authorized users of the system;2. Group and role membership; and3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];g. Monitor the 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 users are terminated or transferred; and3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual;i. Authorize access to the system based on:1. A valid access authorization;2. Intended system usage; and3. [Assignment: organization-defined attributes (as required)];j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; andl. Align account management processes with personnel termination and transfer processes.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5		AC-02	AC-02	AC-02	AC-02	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(01)		AC-02(01)	AC-02(01)	AC-02(01)
AC-02(02)	Account Management | Automated Temporary and Emergency Account Management	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	10					AC-2(2)	AC-2(2)
AC-02(03)	Account Management | Disable Accounts	Disable accounts within [Assignment: organization-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-defined time period].	Functional	Equal	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	10					AC-2(3)	AC-2(3)
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	Automated mechanisms exist to audit account creation, modification, enabling, disabling and removal actions and notify organization-defined personnel or roles.	10					AC-2(4)	AC-2(4)
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	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and	10					AC-2(5)	AC-2(5)
AC-02(07)	Account Management | Privileged User Accounts	a. Establish and administer privileged user accounts in 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 longer appropriate.	Functional	Equal	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business	10		AC-02(07)		AC-02(07)	AC-02(07)	AC-02(07)
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-2(9)	AC-2(9)
AC-02(10)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5				AC-2(10)	AC-2(10)
AC-02(11)	Account Management | Usage Conditions	Enforce [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined system accounts].	Functional	Equal	Usage Conditions	IAC-15.8	Automated mechanisms exist to enforce usage conditions for users and/or roles.	10						AC-2(11)
AC-02(12)	Account Management | Account Monitoring for Atypical Usage	a. Monitor system accounts for [Assignment: organization-defined atypical usage]; andb. Report atypical usage of system accounts to [Assignment: organization-defined personnel or roles].	Functional	Equal	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	10					AC-2(12)	AC-2(12)
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 and/or Data (TAASD) upon termination, as determined by management.	5						AC-2(13)
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-2(13)
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	AC-03	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	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5			AC-03	AC-03	AC-03	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	AC-03	AC-03
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	Mechanisms exist to design, implement and review firewall and router configurations to restrict connections between untrusted networks and internal systems.	10		AC-04		AC-04	AC-04	AC-04

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
AC-04(08)	Information Flow Enforcement | Security and Privacy Policy Filters	a. Enforce information flow control using [Assignment: organization-defined security or privacy policy filters] as a basis for flow control decisions for [Assignment: organization-defined information flows]; andb. [Selection (one or more): Block; Strip; Modify; Quarantine] data after a filter processing failure in accordance with [Assignment: organization-defined security or privacy policy].	Functional	Equal	Policy Decision Point (PDP)	NET-04.7	Automated mechanisms exist to evaluate access requests against established criteria to dynamically and uniformly enforce access rights and permissions.	10						AC-04(08)
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 and/or Services (TAAS) to protect from other network resources.	10					AC-04(21)	AC-04(21)
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	AC-05	AC-05
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 Services (TAAS).	5				AC-05	AC-05	AC-05
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	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5				AC-05	AC-05	AC-05
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-05	AC-05	AC-05
AC-06	Least Privilege	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5		AC-06		AC-06	AC-06	AC-06
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		AC-06	AC-06	AC-06
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-	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(01)	AC-06(01)
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(02)			AC-06(02)	AC-06(02)
AC-06(03)	Least Privilege | Network Access to Privileged Commands	Authorize network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and document the rationale for such access in the security plan for the system.	Functional	Equal	Network Access to Privileged Commands	IAC-21.6	Mechanisms exist to authorize remote access to perform privileged commands on critical Technology Assets, Applications and/or Services (TAAS) or where sensitive/regulated data is stored, transmitted and/or processed only for compelling	10						AC-06(03)
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(05)	AC-06(05)
AC-06(07)	Least Privilege | Review of User Privileges	a. Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; andb. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.	Functional	Equal	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	10						AC-06(07)
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(08)
AC-06(09)	Least Privilege | Log Use of Privileged	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(09)	AC-06(09)
AC-06(10)	Least Privilege | Prohibit Non-privileged Users from Executing Privileged Functions	Prevent non-privileged users from executing privileged functions.	Functional	Equal	Prohibit Non-Privileged Users from Executing Privileged Functions	IAC-21.5	Mechanisms exist to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards /	10		AC-06(10)			AC-06(10)	AC-06(10)
AC-07	Unsuccessful Logon Attempts	a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; andb. Automatically [Selection (one or more): 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 delay algorithm]; notify system administrator; take other [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded.	Functional	Equal	Account Lockout	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	10			AC-07	AC-07	AC-07	AC-07
AC-07(02)	Unsuccessful Logon Attempts | Purge or Wipe Mobile Device	Purge or wipe information from [Assignment: organization-defined mobile devices] based on [Assignment: organization-defined purging or wiping requirements and techniques] after [Assignment: organization-defined number] consecutive, unsuccessful device logon attempts.	Functional	Equal	Remote Purging	MDM-05	Mechanisms exist to remotely purge selected information from mobile devices.	10						AC-07(02)
AC-08	System Use Notification	a. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:1. Users are accessing a U.S. Government system;2. System usage may be monitored, recorded, and subject to audit;3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and4. Use of the system indicates consent to monitoring and recording;b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; andc. For publicly accessible systems:1. Display system use information [Assignment: organization-defined conditions], before granting further access to the publicly accessible system;2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and3. Include a description of the	Functional	Equal	System Use Notification (Logon Banner)	SEA-18	Mechanisms exist to utilize system use notification / logon banners that display an approved system use notification message or banner before granting access to the system that provides cybersecurity and data protection notices.	10			AC-08	AC-08	AC-08	AC-08
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-10	AC-10
AC-11	Device Lock	a. Prevent further access to the system by [Selection (one or more): initiating a device lock after [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 using established identification and authentication procedures.	Functional	Intersects With	Session Lock	IAC-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and	5				AC-11	AC-11	AC-11
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-11(01)	AC-11(01)
AC-12	Session Termination	Automatically terminate a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].	Functional	Equal	Session Termination	IAC-25	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.	10				AC-12	AC-12	AC-12

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
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(01)
AC-14	Permitted Actions Without Identification or Authentication	a. Identify [Assignment: organization-defined user 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 identification or authentication.	Functional	Equal	Permitted Actions Without Identification or Authorization	IAC-26	Mechanisms exist to identify and document the supporting rationale for specific user actions that can be performed on a system without identification or authentication.	10			AC-14	AC-14	AC-14	AC-14
AC-17	Remote Access	a. Establish and document usage restrictions, 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 connections.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5		AC-17	AC-17	AC-17	AC-17	AC-17
AC-17(01)	Remote Access | Monitoring and Control	Employ automated mechanisms to monitor and control remote access methods.	Functional	Equal	Automated Monitoring & Control	NET-14.1	Automated mechanisms exist to monitor and control remote access sessions.	10				AC-17(01)	AC-17(01)	AC-17(01)
AC-17(02)	Remote Access | Protection of Confidentiality and Integrity Using Encryption	Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	Functional	Equal	Protection of Confidentiality / Integrity Using Encryption	NET-14.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).	10		AC-17(02)		AC-17(02)	AC-17(02)	AC-17(02)
AC-17(03)	Remote Access | Managed Access Control Points	Route remote accesses through authorized and managed network access control points.	Functional	Equal	Managed Access Control Points	NET-14.3	Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).	10					AC-17(03)	AC-17(03)
AC-17(04)	Remote Access | Privileged Commands and Access	a. Authorize the execution of privileged commands and 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	Functional	Equal	Remote Privileged Commands & Sensitive Data Access	NET-14.4	Mechanisms exist to restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.	10					AC-17(04)	AC-17(04)
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	10				AC-17(09)	AC-17(09)	AC-17(09)
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	AC-18	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 wireless access via secure authentication and encryption.	5			AC-18	AC-18	AC-18	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 protect wireless access through authentication and strong encryption.	10					AC-18(01)	AC-18(01)
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	Mechanisms exist to disable unnecessary wireless networking capabilities that are internally embedded within system components prior to issuance to end users.	10						AC-18(03)
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(04)
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-18(05)
AC-19	Access Control for Mobile Devices	a. Establish configuration requirements, connection 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 organizational systems.	Functional	Equal	Access Control For Mobile Devices	MDM-02	Mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	10			AC-19	AC-19	AC-19	AC-19
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-19(05)	AC-19(05)
AC-20	Use of External Systems	a. [Selection (one or more): Establish [Assignment: organization-defined terms and conditions]; Identify [Assignment: organization-defined controls asserted to be implemented on external systems]], consistent with 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. Process, store, or transmit organization-controlled information using external systems; orb. Prohibit the use of [Assignment: organizationally-defined types of external systems].	Functional	Equal	Use of External Information Systems	DCH-13	Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.	10			AC-20	AC-20	AC-20	AC-20
AC-20(01)	Use of External Systems | Limits on Authorized Use	Permit authorized individuals to use an external system to access the system or to process, store, or 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 system connection or processing agreements with the organizational entity hosting the external system.	Functional	Equal	Limits of Authorized Use	DCH-13.1	Mechanisms exist to prohibit external parties, including Technology Assets, Applications and/or Services (TAAS), from storing, processing and transmitting data unless authorized individuals first: (1) Verifying the implementation of required security controls; or (2) Retaining a processing agreement with the entity hosting the external TAAS.	10					AC-20(01)	AC-20(01)	AC-20(01)
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(02)	AC-20(02)
AC-21	Information Sharing	a. Enable authorized users to determine whether access authorizations assigned to a sharing partner 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 users in making information sharing and collaboration decisions.	Functional	Intersects With	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose 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 subject.	5					AC-21	AC-21
AC-21	Information Sharing	a. Enable authorized users to determine whether access authorizations assigned to a sharing partner 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 users in making information sharing and collaboration decisions.	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	AC-21
AC-22	Publicly Accessible Content	a. Designate individuals authorized to make information publicly accessible;b. Train authorized individuals to ensure that publicly accessible 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 for nonpublic information [Assignment: organization-defined frequency] and remove such information, if discovered.	Functional	Equal	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	10					AC-22	AC-22

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
AT-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, 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 [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; andc. Review and update the current awareness and training:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5			AT-01	AT-01	AT-01	AT-01
AT-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, 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 [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; andc. Review and update the current awareness and training:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined	Functional	Subset Of	Cybersecurity & Data Protection-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10			AT-01	AT-01	AT-01	AT-01
AT-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, 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 [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; andc. Review and update the current awareness and training:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5			AT-01	AT-01	AT-01	AT-01
AT-02	Literacy Training and Awareness	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):1. As part of initial training for new users and [Assignment: organization-defined frequency] thereafter; and2. When required by system 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 content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; andd. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.	Functional	Equal	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	10			AT-02	AT-02	AT-02	AT-02
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(02)	AT-02(02)
AT-03	Role-based Training	a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined roles and responsibilities]:1 . Before authorizing access to the 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: organization-defined frequency] and following [Assignment: organization-defined events]; andc. Incorporate lessons learned from internal or external security incidents or breaches into role-	Functional	Intersects With	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5			AT-03	AT-03	AT-03	AT-03
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 cybersecurity and data protection training that reinforce training objectives.	10						AT-03(03)
AT-03(04)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5					AT-03(04)
AT-04	Training Records	a. Document and monitor information security and 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 time period].	Functional	Equal	Cybersecurity & Data Protection Training Records	SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including basic cybersecurity and data protection awareness training, ongoing awareness training and specific-	10			AT-04	AT-04	AT-04	AT-04
AU-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, 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: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; andc. Review and update the current audit and accountability:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5			AU-01	AU-01	AU-01	AU-01
AU-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, 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: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; andc. Review and update the current audit and accountability:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5			AU-01	AU-01	AU-01	AU-01

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
AU-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, 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: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; andc. Review and update the current audit and accountability:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10			AU-01	AU-01	AU-01	AU-01
AU-02	Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-02a.) along with the frequency of (or situation requiring) logging for each identified event type];d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; ande. Review and update the event types selected for logging [Assignment: organization-defined	Functional	Intersects With	Reviews & Updates	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5			AU-02	AU-02	AU-02	AU-02
AU-02	Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-02a.) along with the frequency of (or situation requiring) logging for each identified event type];d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; ande. Review and update the event types selected for logging [Assignment: organization-defined	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.	5			AU-02	AU-02	AU-02	AU-02
AU-02(03)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5			AU-02(03)	AU-02(03)	AU-02(03)
AU-03	Content of Audit Records	Ensure that audit records contain information that 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 objects/entities associated with the event.	Functional	Equal	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	10			AU-03	AU-03	AU-03	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 Audit Information	MON-03.1	Mechanisms exist to protect sensitive/regulated data contained in log files.	5					AU-03(01)	AU-03(01)
AU-03(02)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5					AU-03(02)
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	AU-04	AU-04
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	AU-05	AU-05
AU-05(01)	Response to Audit Logging Process Failures | Storage Capacity Warning	Provide a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated audit log storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit log storage capacity.	Functional	Equal	Event Log Storage Capacity Alerting	MON-05.2	Automated mechanisms exist to alert appropriate personnel when the allocated volume reaches an organization-defined percentage of maximum event log storage capacity.	10						AU-05(01)
AU-05(02)	Response to Audit Logging Process Failures | Real-time Alerts	Provide an alert within [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit logging failure events requiring real-time alerts].	Functional	Intersects With	Real-Time Alerts of Event Logging Failure	MON-05.1	Mechanisms exist to provide 24x7x365 near real-time alerting capability when an event log processing failure occurs.	5						AU-05(02)
AU-06	Audit Record Review, Analysis, and Reporting	a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity;b. Report findings to [Assignment: organization-defined personnel or roles]; andc. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.	5			AU-06	AU-06	AU-06	AU-06
AU-06	Audit Record Review, Analysis, and Reporting	a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity;b. Report findings to [Assignment: organization-defined personnel or roles]; andc. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.	Functional	Intersects With	Audit Level Adjustments	MON-02.6	Mechanisms exist to adjust the level of audit review, analysis and reporting based on evolving threat information from law enforcement, industry associations or other credible sources of threat intelligence.	5			AU-06	AU-06	AU-06	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 Audit Information	MON-03.1	Mechanisms exist to protect sensitive/regulated data contained in log files.	5				AU-06(01)	AU-06(01)	AU-06(01)
AU-06(03)	Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories	Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5					AU-06(03)	AU-06(03)
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(04)
AU-06(05)	Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records	Integrate analysis of audit records with analysis of [Selection (one or more): vulnerability scanning information; performance data; system monitoring information; [Assignment: organization-defined data/information collected from other sources]] to further enhance the ability to identify inappropriate or unusual activity.	Functional	Equal	Integration of Scanning & Other Monitoring Information	MON-02.3	Automated mechanisms exist to integrate the analysis of audit records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further enhance the ability to identify inappropriate or unusual activity.	10						AU-06(05)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
AU-06(06)	Audit Record Review, Analysis, and Reporting | Correlation with Physical Monitoring	Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.	Functional	Equal	Correlation with Physical Monitoring	MON-02.4	Automated mechanisms exist to correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual or malevolent activity.	10						AU-06(06)
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 (TAAS) associated with the review, analysis and reporting of audit information.	10						AU-06(07)
AU-06(10)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5					AU-06(10)
AU-07	Audit Record Reduction and Report Generation	Provide and implement an audit record reduction and 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 time ordering of 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			AU-07	AU-07
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(01)			AU-07(01)	AU-07(01)
AU-08	Time Stamps	a. Use internal system clocks to generate 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 the local time offset as part of the time stamp.	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	AU-08	AU-08
AU-08	Time Stamps	a. Use internal system clocks to generate 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 the local time offset as part of the time stamp.	Functional	Intersects With	Time Stamps	MON-07	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to use an authoritative time source to generate time stamps for event logs.	5			AU-08	AU-08	AU-08	AU-08
AU-08(01)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5		AU-08(01)	AU-08(01)	AU-08(01)	AU-08(01)
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	AU-09	AU-09
AU-09(02)	Protection of Audit Information | Store on Separate Physical Systems or Components	Store audit records [Assignment: organization-defined frequency] in a repository that is part of a physically different system or system component than the system or component being audited.	Functional	Intersects With	Event Log Backup on Separate Physical Systems / Components	MON-08.1	Mechanisms exist to back up event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or similar automated tool.	5					AU-09(02)	AU-09(02)
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(03)
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(04)	AU-09(04)
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
AU-11	Audit Record Retention	Retain audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.	Functional	Equal	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	10		AU-11	AU-11	AU-11	AU-11	AU-11
AU-12	Audit Record Generation	a. Provide audit record generation capability for the event types the system is capable of auditing as 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 records for the event types defined in AU-2c that include the audit record	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	AU-12	AU-12
AU-12(01)	Audit Record Generation | System-wide and Time-correlated Audit Trail	Compile audit records from [Assignment: organization-defined system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail].	Functional	Equal	System-Wide / Time-Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.	10						AU-12(01)
AU-12(03)	Audit Record Generation | Changes by Authorized Individuals	Provide and implement the capability for [Assignment: organization-defined individuals or roles] to change the logging to be performed on [Assignment: organization-defined system components] based on [Assignment: organization-defined selectable event criteria] within [Assignment: organization-defined time thresholds].	Functional	Equal	Changes by Authorized Individuals	MON-02.8	Mechanisms exist to provide privileged users or roles the capability to change the auditing to be performed on specified system components, based on specific event criteria within specified time thresholds.	10						AU-12(03)
CA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] assessment, authorization, and monitoring policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, 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-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; andc. Review and update the current assessment, authorization, and monitoring:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection assessment and authorization controls.	10			CA-01	CA-01	CA-01	CA-01
CA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] assessment, authorization, and monitoring policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, 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-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; andc. Review and update the current assessment, authorization, and monitoring:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5			CA-01	CA-01	CA-01	CA-01

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
CA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] assessment, authorization, and monitoring policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, 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-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; andc. Review and update the current assessment, authorization, and monitoring:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5			CA-01	CA-01	CA-01	CA-01
CA-02	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;b. Develop a control assessment plan that describes the scope of the assessment including:1. Controls and control enhancements under assessment;2. Assessment procedures to be used to determine control effectiveness; and3. Assessment environment, assessment team, and assessment roles and responsibilities;c. Ensure the control assessment plan 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: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;e. Produce a control assessment report that document the results of the assessment; andf. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].	Functional	Intersects With	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's cybersecurity and data protection policies and standards.	5			CA-02	CA-02	CA-02	CA-02
CA-02	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;b. Develop a control assessment plan that describes the scope of the assessment including:1. Controls and control enhancements under assessment;2. Assessment procedures to be used to determine control effectiveness; and3. Assessment environment, assessment team, and assessment roles and responsibilities;c. Ensure the control assessment plan 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: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;e. Produce a control assessment report that document the results of the assessment; andf. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical cybersecurity and data protection controls.	5			CA-02	CA-02	CA-02	CA-02
CA-02	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;b. Develop a control assessment plan that describes the scope of the assessment including:1. Controls and control enhancements under assessment;2. Assessment procedures to be used to determine control effectiveness; and3. Assessment environment, assessment team, and assessment roles and responsibilities;c. Ensure the control assessment plan 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: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;e. Produce a control assessment report that document the results of the assessment; andf. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].	Functional	Intersects With	Cybersecurity & Data Protection In Project Management	PRM-04	Mechanisms exist to assess cybersecurity and data protection controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5			CA-02	CA-02	CA-02	CA-02
CA-02	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;b. Develop a control assessment plan that describes the scope of the assessment including:1. Controls and control enhancements under assessment;2. Assessment procedures to be used to determine control effectiveness; and3. Assessment environment, assessment team, and assessment roles and responsibilities;c. Ensure the control assessment plan 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: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;e. Produce a control assessment report that document the results of the assessment; andf. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity and data protection controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5			CA-02	CA-02	CA-02	CA-02
CA-02	Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;b. Develop a control assessment plan that describes the scope of the assessment including:1. Controls and control enhancements under assessment;2. Assessment procedures to be used to determine control effectiveness; and3. Assessment environment, assessment team, and assessment roles and responsibilities;c. Ensure the control assessment plan 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: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;e. Produce a control assessment report that document the results of the assessment; andf. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].	Functional	Intersects With	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate cybersecurity and data protection policies, standards and other applicable requirements.	5			CA-02	CA-02	CA-02	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	Mechanisms exist to ensure assessors or assessment teams have the appropriate independence to conduct cybersecurity and data protection control assessments.	10			CA-02(01)	CA-02(01)	CA-02(01)	CA-02(01)
CA-02(02)	Control Assessments | Specialized Assessments	Include as part of control assessments, [Assignment: organization-defined frequency], [Selection (one): announced; unannounced], [Selection (one or more): in-depth monitoring; security instrumentation; automated security test cases; vulnerability scanning; malicious user testing; insider threat assessment; performance and load testing; data leakage or data loss assessment; [Assignment: organization-defined other forms of assessment]].	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; and/or (11) Artificial Intelligence and Automonous Technologies (AAT).	5						CA-02(02)	CA-02(02)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
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	Functional	Equal	Third-Party Assessments	IAO-02.3	Mechanisms exist to accept and respond to the results of external assessments that are performed by impartial, external organizations.	10					CA-02(03)	CA-02(03)
CA-03	Information Exchange	a. Approve and manage the exchange of information between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements; [Assignment: organization-defined type of agreement]];b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; andc. Review and update the agreements [Assignment: organization-	Functional	Intersects With	System Interconnections	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection, the interface characteristics, cybersecurity and data protection requirements and the nature of the information communicated.	5			CA-03	CA-03	CA-03	CA-03
CA-03(05)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5				CA-03(05)	CA-03(05)
CA-05	Plan of Action and Milestones	a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or 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: organization-defined frequency] based on the findings from control assessments, independent audits or reviews, and continuous monitoring	Functional	Intersects With	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5			CA-05	CA-05	CA-05	CA-05
CA-06	Authorization	a. Assign a senior official as the authorizing official for the system;b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;c. Ensure that the 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 common controls authorizes the use of those controls for inheritance by organizational systems;e. Update the authorizations [Assignment: organization-defined frequency].	Functional	Equal	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	10			CA-06	CA-06	CA-06	CA-06
CA-07	Continuous Monitoring	Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:a. Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics];b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: 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 continuous monitoring strategy;e. Correlation and analysis of information generated by control assessments and monitoring;f. Response actions to address results of the analysis of control assessment and monitoring information; andg. Reporting the security and privacy status of the system to [Assignment: organization-defined personnel or roles] [Assignment:	Functional	Intersects With	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership.	5			CA-07	CA-07	CA-07	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 cybersecurity and data protection controls at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes	5				CA-07(01)	CA-07(01)	CA-07(01)
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	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership.	5				CA-07(01)	CA-07(01)	CA-07(01)
CA-07(03)	Continuous Monitoring | Trend Analyses	Employ trend analyses to determine if control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data.	Functional	Equal	Trend Analysis Reporting	MON-06.2	Mechanisms exist to employ trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on	10						CA-07(03)
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	CA-08	CA-08
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(01)	CA-08(01)	CA-08(01)
CA-09	Internal System Connections	a. Authorize internal connections of [Assignment: organization-defined system components or classes of components] to the system;b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;c. Terminate internal system connections after [Assignment: organization-defined conditions]; andd. Review [Assignment: organization-defined frequency] the continued need for each internal connection.	Functional	Equal	Internal System Connections	NET-05.2	Mechanisms exist to control internal system connections through authorizing internal connections of systems and documenting, for each internal connection, the interface characteristics, security requirements and the nature of the information communicated.	10			CA-09	CA-09	CA-09	CA-09
CM-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, 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 [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; andc. Review and update the current configuration management:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10			CM-01	CM-01	CM-01	CM-01
CM-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, 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 [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; andc. Review and update the current configuration management:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5			CM-01	CM-01	CM-01	CM-01

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
CM-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, 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 [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; andc. Review and update the current configuration management:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5			CM-01	CM-01	CM-01	CM-01
CM-02	Baseline Configuration	a. Develop, document, and maintain under configuration control, a current 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]; and3. When system components are installed or upgraded.	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	5		CM-02	CM-02	CM-02	CM-02	CM-02
CM-02	Baseline Configuration	a. Develop, document, and maintain under configuration control, a current 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]; and3. When system components are installed or upgraded.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening	5		CM-02	CM-02	CM-02	CM-02	CM-02
CM-02(01)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5			CM-02(01)	CM-02(01)	CM-02(01)
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 Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar	10		CM-02(02)			CM-02(02)	CM-02(02)
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(03)	CM-02(03)	CM-02(03)
CM-02(07)	Baseline Configuration | Configure Systems and Components for High-risk Areas	a. Issue [Assignment: organization-defined systems or system components] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; andb. Apply the following controls to the systems or components when the individuals return from travel: [Assignment: organization-defined controls].	Functional	Equal	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	10					CM-02(07)	CM-02(07)
CM-03	Configuration Change Control	a. Determine and document the types of changes to the system that are configuration-controlled;b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;c. Document configuration change decisions associated with the system;d. Implement approved 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 configuration-controlled changes to the system; andg. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10					CM-03	CM-03	CM-03
CM-03	Configuration Change Control	a. Determine and document the types of changes to the system that are configuration-controlled;b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;c. Document configuration change decisions associated with the system;d. Implement approved 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 configuration-controlled changes to the system; andg. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5					CM-03	CM-03	CM-03
CM-03(01)	Configuration Change Control | Automated Documentation, Notification, and Prohibition of Changes	Use [Assignment: organization-defined automated mechanisms] to:a. Document proposed changes to the system;b. Notify [Assignment: organization-defined approval authorities] of proposed changes to the system and request change approval;c. Highlight proposed changes to the system that have not been approved or disapproved within [Assignment: organization-defined time period];d. Prohibit changes to the system until designated approvals are received;e. Document all changes to the system; andf. Notify [Assignment: organization-defined personnel] when approved changes to the system are	Functional	Equal	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	10						CM-03(01)
CM-03(02)	Configuration Change Control | Testing, Validation, and Documentation of Changes	Test, validate, and document changes to the system before finalizing the implementation of the changes.	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of cybersecurity and/or data privacy controls following implemented changes to ensure applicable controls operate as designed.	5				CM-03(02)	CM-03(02)	CM-03(02)
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	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	5				CM-03(02)	CM-03(02)	CM-03(02)
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	Cybersecurity & Data Protection Representative for Asset Lifecycle Changes	CHG-02.3	Mechanisms exist to include a cybersecurity and/or data protection representative in the configuration change control review process.	10						CM-03(04)
CM-03(06)	Configuration Change Control | Cryptography Management	Ensure that cryptographic mechanisms used to provide the following controls are under configuration management: [Assignment: organization-defined controls].	Functional	Equal	Cryptographic Management	CHG-02.5	Mechanisms exist to govern assets involved in providing cryptographic protections according to the organization's configuration management processes.	10						CM-03(06)
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	CM-04	CM-04	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 access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS).	10						CM-04(01)
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 Assets, Applications and/or Services (TAAS).	5		CM-05		CM-05	CM-05	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	CM-05	CM-05

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
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(01)			CM-05(01)	CM-05(01)
CM-05(02)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5					CM-05(02)
CM-05(03)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5				CM-05(03)	CM-05(03)
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(05)			CM-05(05)	CM-05(05)
CM-06	Configuration Settings	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined 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-defined operational requirements]; andd. Monitor and control changes to the configuration settings in accordance with	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5		CM-06	CM-06	CM-06	CM-06	CM-06
CM-06	Configuration Settings	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined 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-defined operational requirements]; andd. Monitor and control changes to the configuration settings in accordance with	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	CM-06	CM-06	CM-06
CM-06(01)	Configuration Settings | Automated Management, Application, and Verification	Manage, apply, and verify configuration settings for [Assignment: organization-defined system components] using [Assignment: organization-defined automated mechanisms].	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar	5		CM-06(01)		CM-06(01)	CM-06(01)	CM-06(01)
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(02)
CM-07	Least Functionality	a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; andb. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].	Functional	Equal	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	10			CM-07	CM-07	CM-07	CM-07
CM-07(01)	Least Functionality | Periodic Review	a. Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; andb. Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure].	Functional	Equal	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	10					CM-07(01)	CM-07(01)
CM-07(02)	Least Functionality | Prevent Program Execution	Prevent program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].	Functional	Intersects With	Prevent Program Execution	SEA-06	Automated mechanisms exist to prevent the execution of unauthorized software programs.	5					CM-07(02)	CM-07(02)
CM-07(02)	Least Functionality | Prevent Program Execution	Prevent program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].	Functional	Intersects With	Prevent Unauthorized Software Execution	CFG-03.2	Mechanisms exist to configure systems to prevent the execution of unauthorized software programs.	5					CM-07(02)	CM-07(02)
CM-07(05)	Least Functionality | Authorized Software — Allow-by-exception	a. Identify [Assignment: organization-defined software programs authorized to execute on the system];b. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; andc. Review and update the list of authorized software programs [Assignment: organization-defined frequency].	Functional	Equal	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	10					CM-07(05)	CM-07(05)
CM-08	System Component Inventory	a. Develop and document an inventory of system components that:1. Accurately reflects the system;2. Includes all components within the system;3. Does not include duplicate accounting of components or 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 necessary to achieve effective system component accountability]; andb. Review and update the system component inventory [Assignment: organization-defined frequency].	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5		CM-08	CM-08	CM-08	CM-08	CM-08
CM-08	System Component Inventory	a. Develop and document an inventory of system components that:1. Accurately reflects the system;2. Includes all components within the system;3. Does not include duplicate accounting of components or 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 necessary to achieve effective system component accountability]; andb. Review and update the system component inventory [Assignment: organization-defined frequency].	Functional	Intersects With	Component Duplication Avoidance	AST-02.3	Mechanisms exist to establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components that prevents assets from being duplicated in other asset inventories.	5		CM-08	CM-08	CM-08	CM-08	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(01)	CM-08(01)	CM-08(01)	CM-08(01)
CM-08(02)	System Component Inventory | Automated Maintenance	Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [Assignment: organization-defined automated mechanisms].	Functional	Equal	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	10						CM-08(02)
CM-08(03)	System Component Inventory | Automated Unauthorized Component Detection	a. Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; andb. Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].	Functional	Intersects With	Automated Unauthorized Component Detection	AST-02.2	Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.	5					CM-08(03)	CM-08(03)
CM-08(03)	System Component Inventory | Automated Unauthorized Component Detection	a. Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; andb. Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].	Functional	Intersects With	Software Installation Alerts	END-03.1	Mechanisms exist to generate an alert when new software is detected.	5					CM-08(03)	CM-08(03)
CM-08(03)	System Component Inventory | Automated Unauthorized Component Detection	a. Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; andb. Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].	Functional	Intersects With	Unauthorized Installation Alerts	CFG-05.1	Mechanisms exist to configure systems to generate an alert when the unauthorized installation of software is detected.	5					CM-08(03)	CM-08(03)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
CM-08(04)	System Component Inventory | Accountability Information	Include in the system component inventory information, a means for identifying by [Selection (one or more): name; position; role], individuals responsible and accountable for administering those components.	Functional	Equal	Accountability Information	AST-03.1	Mechanisms exist to include capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory process.	10						CM-08(04)
CM-08(05)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5				CM-08(05)	CM-08(05)
CM-09	Configuration Management Plan	Develop, document, and implement a configuration management plan for the system that:a. Addresses roles, responsibilities, and configuration management processes and procedures;b. Establishes a process for 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 management;d. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; ande. Protects the configuration management plan from unauthorized disclosure and	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10		CM-09		CM-09	CM-09	CM-09
CM-09	Configuration Management Plan	Develop, document, and implement a configuration management plan for the system that:a. Addresses roles, responsibilities, and configuration management processes and procedures;b. Establishes a process for 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 management;d. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; ande. Protects the configuration management plan from unauthorized disclosure and	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		CM-09	CM-09	CM-09
CM-10	Software Usage Restrictions	a. Use software and associated documentation in accordance with contract agreements and copyright 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 the unauthorized distribution, display, performance, or reproduction of	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	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-10(01)	CM-10(01)
CM-11	User-installed Software	a. Establish [Assignment: organization-defined policies] governing the installation of software by users;b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; andc. Monitor policy compliance [Assignment: organization-defined	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	CM-11	CM-11	CM-11
CM-11	User-installed Software	a. Establish [Assignment: organization-defined policies] governing the installation of software by users;b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; andc. Monitor policy compliance [Assignment: organization-defined	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	CM-11	CM-11
CM-11(01)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5					CM-11(01)
CP-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, 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 [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; andc. Review and update the current contingency planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5			CP-01	CP-01	CP-01	CP-01
CP-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, 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 [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; andc. Review and update the current contingency planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10			CP-01	CP-01	CP-01	CP-01
CP-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, 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 [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; andc. Review and update the current contingency planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5			CP-01	CP-01	CP-01	CP-01
CP-02	Contingency Plan	a. Develop a contingency plan for the system that:1. Identifies essential mission and business functions and associated contingency requirements;2. Provides recovery objectives, restoration priorities, and metrics;3. Addresses contingency roles, responsibilities, assigned individuals with contact information;4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;6. Addresses the sharing of contingency information; and7. Is reviewed and approved by [Assignment: organization-defined personnel or roles];b. Distribute copies of the 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 activities;d. Review the contingency plan for the system [Assignment: organization-defined frequency];e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;f. Communicate contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; andh. Protect the	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10			CP-02	CP-02	CP-02	CP-02

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
CP-02	Contingency Plan	a. Develop a contingency plan for the system that:1. Identifies essential mission and business functions and associated contingency requirements;2. Provides recovery objectives, restoration priorities, and metrics;3. Addresses contingency roles, responsibilities, assigned individuals with contact information;4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;6. Addresses the sharing of contingency information; and7. Is reviewed and approved by [Assignment: organization-defined personnel or roles];b. Distribute copies of the 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 activities;d. Review the contingency plan for the system [Assignment: organization-defined frequency];e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;f. Communicate contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; andh. Protect the	Functional	Intersects With	Ongoing Contingency Planning	BCD-06	Mechanisms exist to keep contingency plans current with business needs, technology changes and feedback from contingency plan testing activities.	5			CP-02	CP-02	CP-02	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(01)	CP-02(01)
CP-02(02)	Contingency Plan | Capacity Planning	Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.	Functional	Equal	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	10					CP-02(02)	CP-02(02)
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	5					CP-02(03)	CP-02(03)
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(03)	CP-02(03)
CP-02(04)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5					CP-02(04)
CP-02(05)	Contingency Plan | Continue Mission and Business Functions	Plan for the continuance of [Selection (one): all; essential] mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.	Functional	Equal	Continue Essential Mission & Business Functions	BCD-02.2	Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration at primary processing and/or storage	10						CP-02(05)
CP-02(08)	Contingency Plan | Identify Critical Assets	Identify critical system assets supporting [Selection (one): all; essential] mission and business functions.	Functional	Equal	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	10				CP-02(08)	CP-02(08)	CP-02(08)
CP-03	Contingency Training	a. Provide contingency training to system users consistent with assigned roles and responsibilities:1. 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 [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	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	CP-03	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(01)	CP-03(01)
CP-04	Contingency Plan Testing	a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests].b. Review the contingency plan test results; andc. Initiate corrective actions, if needed.	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	CP-04	CP-04
CP-04	Contingency Plan Testing	a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests].b. Review the contingency plan test results; andc. Initiate corrective actions, if needed.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5			CP-04	CP-04	CP-04	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(01)	CP-04(01)
CP-04(02)	Contingency Plan Testing | Alternate Processing Site	Test the contingency plan at the alternate processing site:a. To familiarize contingency personnel with the facility and available resources; andb. To evaluate the capabilities of the alternate processing site to support contingency operations.	Functional	Equal	Alternate Storage & Processing Sites	BCD-04.2	Mechanisms exist to test contingency plans at alternate storage & processing sites to both familiarize contingency personnel with the facility and evaluate the capabilities of the alternate processing site to support contingency operations.	10						CP-04(02)
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	Mechanisms exist to establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup	10				CP-06	CP-06	CP-06
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 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(01)	CP-06(01)
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(02)
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	Accessibility	BCD-08.2	Mechanisms exist to identify and mitigate potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.	10					CP-06(03)	CP-06(03)
CP-07	Alternate Processing Site	a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined 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 contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; andc. Provide controls at the alternate processing site that are equivalent to those at the primary site.	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		CP-07	CP-07	CP-07
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 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(01)	CP-07(01)
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	Accessibility	BCD-09.2	Mechanisms exist to identify and mitigate potential accessibility problems to the alternate processing site and possible mitigation actions, in the event of an area-wide disruption or disaster.	10					CP-07(02)	CP-07(02)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
CP-07(03)	Alternate Processing Site | Priority of Service	Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).	Functional	Equal	Alternate Site Priority of Service	BCD-09.3	Mechanisms exist to address priority-of-service provisions in alternate processing and storage sites that support availability requirements, including Recovery Time Objectives (RTOs).	10					CP-07(03)	CP-07(03)
CP-07(04)	Alternate Processing Site | Preparation for Use	Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions.	Functional	Equal	Preparation for Use	BCD-09.4	Mechanisms exist to prepare the alternate processing alternate to support essential missions and business functions so that the alternate site is capable of being used as the primary site.	10						CP-07(04)
CP-08	Telecommunications Services	Establish alternate telecommunications services, including necessary agreements to permit the resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	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		CP-08	CP-08	CP-08
CP-08(01)	Telecommunications Services | Priority of Service Provisions	a. Develop primary and alternate telecommunications service agreements that contain priority-of-service 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 alternate telecommunications services are provided by a common carrier.	Functional	Equal	Telecommunications Priority of Service Provisions	BCD-10.1	Mechanisms exist to formalize primary and alternate telecommunications service agreements contain priority-of-service provisions that support availability requirements, including Recovery Time Objectives (RTOs).	10		CP-08(01)			CP-08(01)	CP-08(01)
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	5		CP-08(02)			CP-08(02)	CP-08(02)
CP-08(03)	Telecommunications Services | Separation of Primary and Alternate Providers	Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.	Functional	Equal	Separation of Primary / Alternate Providers	BCD-10.2	Mechanisms exist to obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.	10						CP-08(03)
CP-08(04)	Telecommunications Services | Provider Contingency Plan	a. Require primary and alternate telecommunications service providers to have contingency plans;b. Review provider contingency plans to ensure that the plans meet organizational contingency requirements; andc. Obtain evidence of contingency testing and training by providers [Assignment: organization-defined frequency].	Functional	Equal	Provider Contingency Plan	BCD-10.3	Mechanisms exist to contractually-require external service providers to have contingency plans that meet organizational contingency requirements.	10						CP-08(04)
CP-09	System Backup	a. Conduct backups of user-level information contained in [Assignment: organization-defined system components] [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];c. Conduct backups of system documentation, including security- and privacy-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; andd. Protect the confidentiality, integrity, and availability of backup information.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		CP-09	CP-09	CP-09	CP-09	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 availability of the data.	10				CP-09(01)	CP-09(01)	CP-09(01)
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(02)
CP-09(03)	System Backup | Separate Storage for Critical Information	Store backup copies of [Assignment: organization-defined critical system software and other security-related information] in a separate facility or in a fire rated container that is not collocated with the operational system.	Functional	Equal	Separate Storage for Critical Information	BCD-11.2	Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up.	10					CP-09(03)	CP-09(03)
CP-09(05)	System Backup | Transfer to Alternate Storage Site	Transfer system backup information to the alternate storage site [Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives].	Functional	Equal	Transfer to Alternate Storage Site	BCD-11.6	Mechanisms exist to transfer backup data to the alternate storage site at a rate that is capable of meeting both Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	10						CP-09(05)
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	Information System Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise	5		CP-10	CP-10	CP-10	CP-10	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, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR)	5		CP-10	CP-10	CP-10	CP-10	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	CP-10	CP-10	CP-10
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 Technology Assets, Applications and/or Services (TAAS) in accordance with Recovery Point	10				CP-10(02)	CP-10(02)	CP-10(02)
CP-10(04)	System Recovery and Reconstitution | Restore Within Time Period	Provide the capability to restore system components within [Assignment: organization-defined restoration time periods] from configuration-controlled and integrity-protected information representing a known, operational state for the components.	Functional	Equal	Restore Within Time Period	BCD-12.4	Mechanisms exist to restore Technology Assets, Applications, Services and/or Data (TAASD) within organization-defined restoration time-periods from configuration-controlled and integrity-protected information; representing a known, operational	10						CP-10(04)
IA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; andc. Review and update the current identification and authentication:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5			IA-01	IA-01	IA-01	IA-01

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
IA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; andc. Review and update the current identification and authentication:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined	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	IA-01	IA-01
IA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; andc. Review and update the current identification and authentication:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5			IA-01	IA-01	IA-01	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	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	10		IA-02	IA-02	IA-02	IA-02	IA-02
IA-02(01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	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; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	5		IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)
IA-02(01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	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)	IA-02(01)	IA-02(01)	IA-02(01)
IA-02(01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Information Assurance Enabled Products	TDA-02.2	Mechanisms exist to limit the use of commercially-provided Information Assurance (IA) and IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated or NSA-	5		IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)
IA-02(01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.	Functional	Intersects With	Out-of-Band Multi-Factor Authentication	IAC-06.4	Mechanisms exist to implement Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.	5		IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)	IA-02(01)
IA-02(01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	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)	IA-02(01)	IA-02(01)	IA-02(01)
IA-02(01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	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)	IA-02(01)	IA-02(01)	IA-02(01)
IA-02(01)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	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(01)	IA-02(01)	IA-02(01)	IA-02(01)
IA-02(02)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Information Assurance Enabled Products	TDA-02.2	Mechanisms exist to limit the use of commercially-provided Information Assurance (IA) and IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated or NSA-	5					IA-02(02)	IA-02(02)
IA-02(02)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	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)
IA-02(02)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.	Functional	Intersects With	Out-of-Band Multi-Factor Authentication	IAC-06.4	Mechanisms exist to implement Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.	5					IA-02(02)	IA-02(02)
IA-02(02)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	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)
IA-02(02)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	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)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
IA-02(02)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	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; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	5					IA-02(02)	IA-02(02)
IA-02(02)	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	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(02)
IA-02(03)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5				IA-02(03)	IA-02(03)
IA-02(04)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5					IA-02(04)
IA-02(05)	Identification and Authentication (organizational Users) | Individual Authentication with Group Authentication	When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.	Functional	Equal	Group Authentication	IAC-02.1	Mechanisms exist to require individuals to be authenticated with an individual authenticator when a group authenticator is utilized.	10					IA-02(05)	IA-02(05)
IA-02(08)	Identification and Authentication (organizational Users) | Access to Accounts — Replay Resistant	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(08)
IA-02(09)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5					IA-02(09)
IA-02(11)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5			IA-02(11)	IA-02(11)	IA-02(11)
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(12)
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	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	5					IA-03	IA-03
IA-04	Identifier Management	Manage system identifiers by:a. Receiving authorization from [Assignment: organization-defined 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; andd. Preventing reuse of identifiers for [Assignment: organization-defined time period].	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5		IA-04	IA-04	IA-04	IA-04	IA-04
IA-04	Identifier Management	Manage system identifiers by:a. Receiving authorization from [Assignment: organization-defined 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; andd. Preventing reuse of identifiers for [Assignment: organization-defined time period].	Functional	Intersects With	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).	5		IA-04	IA-04	IA-04	IA-04	IA-04
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	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5		IA-04(04)			IA-04(04)	IA-04(04)
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	5		IA-04(04)			IA-04(04)	IA-04(04)
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(04)			IA-04(04)	IA-04(04)
IA-05	Authenticator Management	Manage system authenticators by:a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;b. Establishing initial authenticator content for any authenticators issued by the organization;c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;d. Establishing and implementing administrative 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-defined time period by authenticator type] or when [Assignment: organization-defined events] occur;g. Protecting authenticator content from unauthorized disclosure and modification;h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; andi. Changing authenticators for group or role accounts when membership to	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	IA-05	IA-05	IA-05
IA-05(01)	Authenticator Management | Password-based Authentication	For password-based authentication:a. Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised 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 immediate selection of a new password upon account recovery;f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;g. Employ automated tools to assist the user in selecting strong password authenticators; andh. Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].	Functional	Intersects With	Automated Support For Password Strength	IAC-10.4	Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.	5		IA-05(01)	IA-05(01)	IA-05(01)	IA-05(01)	IA-05(01)
IA-05(01)	Authenticator Management | Password-based Authentication	For password-based authentication:a. Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised 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 immediate selection of a new password upon account recovery;f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;g. Employ automated tools to assist the user in selecting strong password authenticators; andh. Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].	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)	IA-05(01)	IA-05(01)	IA-05(01)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
IA-05(01)	Authenticator Management | Password-based Authentication	For password-based authentication:a. Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised 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 immediate selection of a new password upon account recovery;f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;g. Employ automated tools to assist the user in selecting strong password authenticators; andh. Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.	5		IA-05(01)	IA-05(01)	IA-05(01)	IA-05(01)	IA-05(01)
IA-05(02)	Authenticator Management | Public Key-based Authentication	a. For public key-based authentication:1. Enforce authorized access to the corresponding private key; and2. Map the authenticated identity to the account of 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 status information; and2. Implement a local cache of revocation data to support path discovery and validation.	Functional	Equal	PKI-Based Authentication	IAC-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	10					IA-05(02)	IA-05(02)
IA-05(03)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5				IA-05(03)	IA-05(03)
IA-05(04)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5				IA-05(04)	IA-05(04)
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(06)	IA-05(06)
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(07)	IA-05(07)
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(08)
IA-05(11)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5		IA-05(11)	IA-05(11)	IA-05(11)	IA-05(11)
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(13)
IA-06	Authentication Feedback	Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.	Functional	Equal	Authenticator Feedback	IAC-11	Mechanisms exist to obscure the feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	10			IA-06	IA-06	IA-06	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	IA-07	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	Cryptographic Module Authentication	CRY-02	Automated mechanisms exist to enable systems to authenticate to a cryptographic module.	5			IA-07	IA-07	IA-07	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	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	10		IA-08			IA-08	IA-08
IA-08(01)	Identification and Authentication (non-organizational Users) | Acceptance of PIV Credentials from Other Agencies	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 Authenticators	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)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5					IA-08(03)
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)
IR-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 official] to manage the development, documentation, and dissemination of the incident response policy and procedures; andc. Review and update the current incident response:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5			IR-01	IR-01	IR-01	IR-01
IR-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 official] to manage the development, documentation, and dissemination of the incident response policy and procedures; andc. Review and update the current incident response:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10			IR-01	IR-01	IR-01	IR-01

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
IR-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 official] to manage the development, documentation, and dissemination of the incident response policy and procedures; andc. Review and update the current incident response:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	5			IR-01	IR-01	IR-01	IR-01
IR-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 official] to manage the development, documentation, and dissemination of the incident response policy and procedures; andc. Review and update the current incident response:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5			IR-01	IR-01	IR-01	IR-01
IR-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 official] to manage the development, documentation, and dissemination of the incident response policy and procedures; andc. Review and update the current incident response:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5			IR-01	IR-01	IR-01	IR-01
IR-02	Incident Response Training	a. Provide incident response training to system users consistent with assigned roles and responsibilities:1. Within [Assignment: organization-defined time period] 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 update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	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	IR-02	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	10						IR-02(01)
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	10						IR-02(02)
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	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5		IR-03	IR-03	IR-03	IR-03	IR-03
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(02)	IR-03(02)
IR-04	Incident Handling	a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;b. Coordinate 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 resulting changes accordingly; andd. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.	Functional	Equal	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10		IR-04	IR-04	IR-04	IR-04	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(01)			IR-04(01)	IR-04(01)
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(02)
IR-04(03)	Incident Handling | Continuity of Operations	Identify [Assignment: organization-defined classes of incidents] and take the following actions in response to those incidents to ensure continuation of organizational mission and business functions: [Assignment: organization-defined actions to take in response to classes of incidents].	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR)	5						IR-04(03)
IR-04(03)	Incident Handling | Continuity of Operations	Identify [Assignment: organization-defined classes of incidents] and take the following actions in response to those incidents to ensure continuation of organizational mission and business functions: [Assignment: organization-defined actions to take in response to classes of incidents].	Functional	Intersects With	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	5						IR-04(03)
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(06)
IR-04(08)	Incident Handling | Correlation with External Organizations	Coordinate with [Assignment: organization-defined external organizations] to correlate and share [Assignment: organization-defined incident information] to achieve a cross-organization perspective on incident awareness and more effective incident responses.	Functional	Equal	Correlation with External Organizations	IRO-02.5	Mechanisms exist to coordinate with approved third-parties to achieve a cross-organization perspective on incident awareness and more effective incident responses.	10						IR-04(08)
IR-05	Incident Monitoring	Track and document incidents.	Functional	Equal	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	10			IR-05	IR-05	IR-05	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	Automated mechanisms exist to assist in the tracking, collection and analysis of information from actual and potential cybersecurity and data protection incidents.	10						IR-05(01)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
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	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and	5		IR-06	IR-06	IR-06	IR-06	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	IR-06	IR-06	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	IR-06	IR-06	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(01)			IR-06(01)	IR-06(01)
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 and/or Services (TAAS) for the handling and reporting of actual and potential cybersecurity and data protection incidents.	10			IR-07	IR-07	IR-07	IR-07
IR-07(01)	Incident Response 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(01)	IR-07(01)
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-07(02)	IR-07(02)	IR-07(02)
IR-08	Incident Response Plan	a. Develop an incident response plan that:1. Provides the organization with a roadmap for implementing its incident response capability;2. Describes the structure and organization of the incident response capability;3. Provides a high-level approach for how the incident response capability fits into the overall organization;4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;5. Defines reportable incidents;6. Provides metrics for measuring the incident response capability within the organization;7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;8. 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: organization-defined entities, personnel, or roles].b. Distribute copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements];c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;d. Communicate incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; ande. Protect the incident response plan from unauthorized disclosure	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	IR-08	IR-08	IR-08
IR-09	Information Spillage Response	Respond to information spills by:a. Assigning [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills;b. Identifying the specific information involved in the system contamination;c. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill;d. Isolating the contaminated system or system component;e. Eradicating the information from the contaminated system or component;f. Identifying other systems or system components that may have been subsequently contaminated; andg. Performing the following additional actions: [Assignment: organization-defined actions].	Functional	Intersects With	Information Spillage Response	IRO-12	Mechanisms exist to respond to sensitive information spills.	5				IR-09	IR-09	IR-09
IR-09	Information Spillage Response	Respond to information spills by:a. Assigning [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills;b. Identifying the specific information involved in the system contamination;c. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill;d. Isolating the contaminated system or system component;e. Eradicating the information from the contaminated system or component;f. Identifying other systems or system components that may have been subsequently contaminated; andg. Performing the following additional actions: [Assignment: organization-defined actions].	Functional	Intersects With	Responsible Personnel	IRO-12.1	Mechanisms exist to formally assign personnel or roles with responsibility for responding to sensitive information spills.	5				IR-09	IR-09	IR-09
IR-09(01)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5			IR-09(01)	IR-09(01)	IR-09(01)
IR-09(02)	Information Spillage Response | Training	Provide information spillage response training [Assignment: organization-defined frequency].	Functional	Equal	Training	IRO-12.2	Mechanisms exist to ensure incident response training material provides coverage for sensitive information spillage response.	10					IR-09(02)	IR-09(02)
IR-09(03)	Information Spillage Response | Post-spill Operations	Implement the following procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions: [Assignment: organization-defined procedures].	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 out assigned tasks while contaminated Technology Assets, Applications and/or Services (TAAS) are undergoing corrective	10					IR-09(03)	IR-09(03)
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	Exposure to Unauthorized Personnel	IRO-12.4	Mechanisms exist to address security safeguards for personnel exposed to sensitive information that is not within their assigned access authorizations.	10					IR-09(04)	IR-09(04)
MA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; andc. Review and update the current maintenance:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment:	Functional	Subset Of	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	10			MA-01	MA-01	MA-01	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 Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
MA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; andc. Review and update the current maintenance:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment:	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	MA-01	MA-01
MA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; andc. Review and update the current maintenance:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment:	Functional	Intersects With	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	5			MA-01	MA-01	MA-01	MA-01
MA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; andc. Review and update the current maintenance:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment:	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5			MA-01	MA-01	MA-01	MA-01
MA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] maintenance policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; andc. Review and update the current maintenance:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment:	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5			MA-01	MA-01	MA-01	MA-01
MA-02	Controlled Maintenance	a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;c. Require that [Assignment: organization-defined 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 removal from organizational facilities for off-site maintenance, repair, or replacement: [Assignment: organization-defined information];e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; andf. Include the following information in organizational maintenance records: [Assignment: organization-defined information].	Functional	Equal	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).	10			MA-02	MA-02	MA-02	MA-02
MA-02(02)	Controlled Maintenance | Automated Maintenance Activities	a. Schedule, conduct, and document maintenance, repair, and replacement actions for the system using [Assignment: organization-defined automated mechanisms]; andb. Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.	Functional	Equal	Automated Maintenance Activities	MNT-02.1	Automated mechanisms exist to schedule, conduct and document maintenance and repairs.	10						MA-02(02)
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		MA-03	MA-03	MA-03
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	10				MA-03(01)	MA-03(01)	MA-03(01)
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(02)	MA-03(02)
MA-03(03)	Maintenance Tools | Prevent Unauthorized Removal	Prevent the removal of maintenance equipment containing organizational information by:a. Verifying 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] explicitly authorizing removal of the equipment from the facility.	Functional	Equal	Prevent Unauthorized Removal	MNT-04.3	Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational information.	10					MA-03(03)	MA-03(03)
MA-04	Nonlocal Maintenance	a. Approve and monitor nonlocal maintenance and diagnostic activities;b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent 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 records for nonlocal maintenance and diagnostic activities; ande. Terminate session and network connections when nonlocal maintenance is	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	MA-04	MA-04
MA-04	Nonlocal Maintenance	a. Approve and monitor nonlocal maintenance and diagnostic activities;b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent 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 records for nonlocal maintenance and diagnostic activities; ande. Terminate session and network connections when nonlocal maintenance is	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	MA-04	MA-04

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
MA-04	Nonlocal Maintenance	a. Approve and monitor nonlocal maintenance and diagnostic activities;b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent 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 records for nonlocal maintenance and diagnostic activities; ande. Terminate session and network connections when nonlocal maintenance is	Functional	Intersects With	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.	5			MA-04	MA-04	MA-04	MA-04
MA-04(02)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5				MA-04(02)	MA-04(02)
MA-04(03)	Nonlocal Maintenance | Comparable Security and Sanitization	a. Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; orb. Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.	Functional	Equal	Remote Maintenance Comparable Security & Sanitization	MNT-05.6	Mechanisms exist to require Technology Assets, Applications and/or Services (TAAS) performing remote, non-local maintenance and/or diagnostic services implement a security capability comparable to the capability implemented on the system being serviced.	10							MA-04(03)
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(06)
MA-05	Maintenance Personnel	a. Establish a process for maintenance personnel authorization and maintain a list of authorized 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 supervise the maintenance activities of personnel who do not possess the required access authorizations.	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	MA-05	MA-05
MA-05(01)	Maintenance Personnel | Individuals Without Appropriate Access	a. Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; and2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; andb. Develop and implement [Assignment: organization-defined alternate controls] in the event a system component cannot be sanitized, removed, or disconnected from	Functional	Intersects With	Maintenance Personnel Without Appropriate Access	MNT-06.1	Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.	5						MA-05(01)	MA-05(01)
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 Services (TAAS) within a defined Recovery Time	10				MA-06	MA-06	MA-06
MP-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] media protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 official] to manage the development, documentation, and dissemination of the media protection policy and procedures; andc. Review and update the current media protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5			MP-01	MP-01	MP-01	MP-01
MP-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] media protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 official] to manage the development, documentation, and dissemination of the media protection policy and procedures; andc. Review and update the current media protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10			MP-01	MP-01	MP-01	MP-01
MP-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] media protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 official] to manage the development, documentation, and dissemination of the media protection policy and procedures; andc. Review and update the current media protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5			MP-01	MP-01	MP-01	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	MP-02	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	MP-02	MP-02
MP-03	Media Marking	a. Mark system media indicating the distribution 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 [Assignment: organization-defined controlled areas].	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5				MP-03	MP-03	MP-03
MP-03	Media Marking	a. Mark system media indicating the distribution 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 [Assignment: organization-defined controlled areas].	Functional	Intersects With	Automated Marking	DCH-04.1	Automated mechanisms exist to mark physical media and digital files to indicate the distribution limitations, handling requirements and applicable security markings (if any) of the information to aid Data Loss Prevention (DLP) technologies.	5				MP-03	MP-03	MP-03

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
MP-04	Media Storage	a. Physically control and securely store [Assignment: 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 procedures.	Functional	Equal	Media Storage	DCH-06	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and	10				MP-04	MP-04	MP-04
MP-05	Media Transport	a. Protect and control [Assignment: organization-defined types of system media] during 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. Restrict the activities associated with the transport of system media to authorized	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	MP-05	MP-05
MP-05(04)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5				MP-05(04)	MP-05(04)
MP-06	Media Sanitization	a. Sanitize [Assignment: organization-defined system 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 security category or classification of the information.	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	MP-06	MP-06
MP-06	Media Sanitization	a. Sanitize [Assignment: organization-defined system 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 security category or classification of the information.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5			MP-06	MP-06	MP-06	MP-06
MP-06	Media Sanitization	a. Sanitize [Assignment: organization-defined system 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 security category or classification of the information.	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	MP-06	MP-06
MP-06(01)	Media Sanitization | Review, Approve, Track, Document, and	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(01)	MP-06(01)	MP-06(01)
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(02)	MP-06(02)
MP-06(03)	Media Sanitization | Nondestructive Techniques	Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage	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)
MP-06(03)	Media Sanitization | Nondestructive Techniques	Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices].	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5						MP-06(03)
MP-06(03)	Media Sanitization | Nondestructive Techniques	Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage	Functional	Intersects With	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).	5						MP-06(03)
MP-07	Media Use	a. [Selection (one): Restrict; Prohibit] the use of [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 when such devices have no identifiable owner.	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	a. [Selection (one): Restrict; Prohibit] the use of [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 when such devices have no identifiable owner.	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	a. [Selection (one): Restrict; Prohibit] the use of [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 when such devices have no identifiable owner.	Functional	Intersects With	Prohibit Use Without Owner	DCH-10.2	Mechanisms exist to prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.	5						MP-07
MP-07(01)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5					MP-07(01)
PE-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. 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-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; andc. Review and update the current physical and environmental protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment:	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5			PE-01	PE-01	PE-01	PE-01
PE-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. 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-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; andc. Review and update the current physical and environmental protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment:	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	PE-01	PE-01
PE-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. 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-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; andc. Review and update the current physical and environmental protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment:	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5			PE-01	PE-01	PE-01	PE-01

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
PE-02	Physical Access Authorizations	a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system 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 individuals from the facility access list when access is no longer	Functional	Equal	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	10			PE-02	PE-02	PE-02	PE-02
PE-03	Physical Access Control	a. Enforce physical access authorizations at [Assignment: organization-defined entry and exit points to the facility where the system resides] by:1. Verifying individual access authorizations before granting access to the facility; and2. Controlling ingress and egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems or devices]; guards];b. Maintain physical access audit logs for [Assignment: organization-defined entry or exit points];c. 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 circumstances requiring visitor escorts and control of visitor activity];e. Secure keys, combinations, and other physical access devices;f. Inventory [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; andg. Change combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5			PE-03	PE-03	PE-03	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 data, in addition to the physical access controls for the facility.	10						PE-03(01)
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	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception,	10				PE-04	PE-04	PE-04
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	Physical security mechanisms exist to restrict access to printers and other system output devices to prevent unauthorized individuals from obtaining the output.	10				PE-05	PE-05	PE-05
PE-06	Monitoring Physical Access	a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; andc. Coordinate results of reviews and investigations with the organizational incident response capability.	Functional	Equal	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	10			PE-06	PE-06	PE-06	PE-06
PE-06(01)	Monitoring Physical Access | Intrusion Alarms and Surveillance	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(01)	PE-06(01)
PE-06(04)	Monitoring Physical Access | Monitoring Physical Access to Systems	Monitor physical access to the system in addition to the physical access monitoring of the facility at [Assignment: organization-defined physical spaces containing one or more components of the system].	Functional	Equal	Monitoring Physical Access To Critical Systems	PES-05.2	Facility security mechanisms exist to monitor physical access to critical systems or sensitive/regulated data, in addition to the physical access monitoring of the facility.	10						PE-06(04)
PE-08	Visitor Access Records	a. Maintain visitor access records to the facility where 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 [Assignment: organization-defined	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	PE-08	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(01)
PE-09	Power Equipment and Cabling	Protect power equipment and power cabling for the system from damage and destruction.	Functional	Equal	Supporting Utilities	PES-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	10					PE-09	PE-09
PE-10	Emergency Shutoff	a. Provide the capability of shutting off power to [Assignment: organization-defined system or individual 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 personnel; andc. Protect emergency power shutoff capability from unauthorized activation.	Functional	Equal	Emergency Shutoff	PES-07.2	Facility security mechanisms exist to shut off power in emergency situations by: (1) Placing emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel; and (2) Protecting emergency power	10					PE-10	PE-10
PE-11	Emergency Power	Provide an uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the system; transition of the system to long-term alternate power] in the event of a primary power source loss.	Functional	Intersects With	Emergency Power	PES-07.3	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.	5					PE-11	PE-11
PE-11(01)	Emergency Power | Alternate Power Supply — Minimal Operational Capability	Provide an alternate power supply for the system that is activated [Selection (one): manually; automatically] and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.	Functional	Intersects With	Emergency Power	PES-07.3	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.	5						PE-11(01)
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	Facility security mechanisms exist to utilize and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the	10					PE-12	PE-12
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	Facility security mechanisms exist to utilize and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.	10			PE-13	PE-13	PE-13	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	Facility security mechanisms exist to utilize and maintain fire detection devices/systems that activate automatically and notify organizational personnel and emergency responders in the event of a fire.	10						PE-13(01)
PE-13(02)	Fire Protection | Suppression Systems — Automatic Activation and Notification	a. Employ fire suppression systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders];andb. Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.	Functional	Intersects With	Automatic Fire Suppression	PES-08.3	Facility security mechanisms exist to employ an automatic fire suppression capability for critical systems when the facility is not staffed on a continuous basis.	5					PE-13(02)	PE-13(02)
PE-13(02)	Fire Protection | Suppression Systems — Automatic Activation and Notification	a. Employ fire suppression systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders];andb. Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.	Functional	Intersects With	Fire Suppression Devices	PES-08.2	Facility security mechanisms exist to utilize fire suppression devices/systems that provide automatic notification of any activation to organizational personnel	5					PE-13(02)	PE-13(02)
PE-13(03)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5				PE-13(03)	PE-13(03)
PE-14	Environmental Controls	a. Maintain [Selection (one or more): temperature; humidity; pressure; radiation; [Assignment: organization-defined environmental control]] levels within the facility where the system resides at [Assignment: organization-defined acceptable levels]; andb. Monitor environmental control levels [Assignment: organization-defined frequency].	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	PE-14	PE-14
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	Facility security mechanisms exist to trigger an alarm or notification of temperature and humidity changes that be potentially harmful to personnel or equipment.	10					PE-14(02)	PE-14(02)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
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	Facility security mechanisms exist to protect systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly and known to key personnel.	10			PE-15	PE-15	PE-15	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 maintenance and IT personnel.	10						PE-15(01)
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	Physical security mechanisms exist to isolate information processing facilities from points such as delivery and loading areas and other points to avoid unauthorized access.	10			PE-16	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	a. Determine and document the [Assignment: organization-defined alternate work sites] allowed for use by employees;b. Employ the following controls at alternate work sites: [Assignment: organization-defined controls];c. Assess the effectiveness of controls at alternate work sites; andd. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.	Functional	Equal	Alternate Work Site	PES-11	Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.	10				PE-17	PE-17	PE-17
PE-18	Location of System Components	Position system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access.	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5						PE-18
PL-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 the development, documentation, and dissemination of the planning policy and procedures; andc. Review and update the current planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined	Functional	Subset Of	Cybersecurity & Data Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection-related resource planning controls that define a viable plan for achieving cybersecurity and data protection objectives.	10			PL-01	PL-01	PL-01	PL-01
PL-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 the development, documentation, and dissemination of the planning policy and procedures; andc. Review and update the current planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined	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	PL-01	PL-01
PL-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 the development, documentation, and dissemination of the planning policy and procedures; andc. Review and update the current planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10			PL-01	PL-01	PL-01	PL-01
PL-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 the development, documentation, and dissemination of the planning policy and procedures; andc. Review and update the current planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5			PL-01	PL-01	PL-01	PL-01
PL-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 the development, documentation, and dissemination of the planning policy and procedures; andc. Review and update the current planning:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5			PL-01	PL-01	PL-01	PL-01

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
PL-02	System Security and Privacy Plans	a. Develop security and privacy plans for the system that: 1. Are consistent with the organization's enterprise architecture;2. Explicitly define the constituent system components;3. Describe the operational context of the system in terms of mission and business processes;4. Identify the individuals that fulfill system roles and responsibilities;5. Identify the information types processed, stored, and transmitted by the system;6. Provide the security categorization of the system, including supporting rationale;7. Describe any specific threats to the system that are of concern to the organization;8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;10. Provide an overview of the security 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 decisions;13. Include risk determinations for security and privacy architecture and design decisions;14. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; and15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles];c. Review the plans [Assignment: organization-defined frequency];d. Update the plans to address changes to the system and environment of operation or problems identified during plan	Functional	Intersects With	Plan / Coordinate with Other Organizational Entities	IAO-03.1	Mechanisms exist to plan and coordinate Information Assurance Program (IAP) activities with affected stakeholders before conducting such activities in order to reduce the potential impact on operations.	5			PL-02	PL-02	PL-02	PL-02
PL-02	System Security and Privacy Plans	a. Develop security and privacy plans for the system that: 1. Are consistent with the organization's enterprise architecture;2. Explicitly define the constituent system components;3. Describe the operational context of the system in terms of mission and business processes;4. Identify the individuals that fulfill system roles and responsibilities;5. Identify the information types processed, stored, and transmitted by the system;6. Provide the security categorization of the system, including supporting rationale;7. Describe any specific threats to the system that are of concern to the organization;8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;10. Provide an overview of the security 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 decisions;13. Include risk determinations for security and privacy architecture and design decisions;14. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; and15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles];c. Review the plans [Assignment: organization-defined frequency];d. Update the plans to address changes to the system and environment of operation or problems identified during plan	Functional	Intersects With	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical Technology Assets, Applications and/or Services (TAAS), as well as influence inputs, entities and TAAS, providing a historical record of the data and its origins.	5			PL-02	PL-02	PL-02	PL-02
PL-02	System Security and Privacy Plans	a. Develop security and privacy plans for the system that: 1. Are consistent with the organization's enterprise architecture;2. Explicitly define the constituent system components;3. Describe the operational context of the system in terms of mission and business processes;4. Identify the individuals that fulfill system roles and responsibilities;5. Identify the information types processed, stored, and transmitted by the system;6. Provide the security categorization of the system, including supporting rationale;7. Describe any specific threats to the system that are of concern to the organization;8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;10. Provide an overview of the security 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 decisions;13. Include risk determinations for security and privacy architecture and design decisions;14. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; and15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles];c. Review the plans [Assignment: organization-defined frequency];d. Update the plans to address changes to the system and environment of operation or problems identified during plan	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	5			PL-02	PL-02	PL-02	PL-02
PL-02(03)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5				PL-02(03)	PL-02(03)
PL-04	Rules of Behavior	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;b. Receive a documented acknowledgment from such individuals, 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]; andd. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more): [Assignment: organization-defined frequency]; when the rules are revised or updated].	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work.	5			PL-04	PL-04	PL-04	PL-04
PL-04	Rules of Behavior	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;b. Receive a documented acknowledgment from such individuals, 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]; andd. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more): [Assignment: organization-defined frequency]; when the rules are revised or updated].	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5			PL-04	PL-04	PL-04	PL-04
PL-04	Rules of Behavior	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;b. Receive a documented acknowledgment from such individuals, 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]; andd. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more): [Assignment: organization-defined frequency]; when the rules are revised or updated].	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	5			PL-04	PL-04	PL-04	PL-04

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
PL-04(01)	Rules of Behavior | Social Media and External Site/application Usage Restrictions	Include in the rules of behavior, restrictions on:a. Use of social media, social networking sites, and external 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 external sites/applications.	Functional	Equal	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	10					PL-04(01)	PL-04(01)
PL-08	Security and Privacy Architectures	a. Develop security and privacy architectures for the system that:1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to 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. Review and update the architectures [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture; andc. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity and data protection principles that addresses risk to organizational operations, assets, individuals, other organizations.	5				PL-08	PL-08	PL-08
PS-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel security policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, 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: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; andc. Review and update the current personnel security:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5			PS-01	PS-01	PS-01	PS-01
PS-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel security policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, 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: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; andc. Review and update the current personnel security:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5			PS-01	PS-01	PS-01	PS-01
PS-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel security policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, 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: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; andc. Review and update the current personnel security:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10			PS-01	PS-01	PS-01	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
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	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5					PS-02	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	PS-03	PS-03
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 additional personnel screening criteria].	Functional	Intersects With	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5						PS-03(03)
PS-04	Personnel Termination	Upon termination of individual employment:a. Disable system access within [Assignment: organization-defined time period];b. Terminate or revoke any authenticators and credentials associated with the individual;c. Conduct exit interviews that include a discussion of [Assignment: organization-defined information security topics];d. Retrieve all security-related organizational system-related property; ande. Retain access to organizational information and systems formerly controlled by terminated individual.	Functional	Equal	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	10			PS-04	PS-04	PS-04	PS-04
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	Automated mechanisms exist to notify Identity and Access Management (IAM) personnel or roles upon termination of an individual employment or contract.	10						PS-04(02)
PS-05	Personnel Transfer	a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities 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 authorization as needed to correspond with any changes in operational need due to reassignment or transfer; andd. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-	Functional	Equal	Personnel Transfer	HRS-08	Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.	10			PS-05	PS-05	PS-05	PS-05
PS-06	Access Agreements	a. Develop and document access agreements for organizational systems;b. Review and update the access agreements [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 maintain access to organizational systems when access agreements have been updated or [Assignment: organization-defined frequency].	Functional	Intersects With	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	5			PS-06	PS-06	PS-06	PS-06

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
PS-06	Access Agreements	a. Develop and document access agreements for organizational systems;b. Review and update the access agreements [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 maintain access to organizational systems when access agreements have been updated or [Assignment: organization-defined frequency].	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	PS-06	PS-06
PS-07	External Personnel Security	a. Establish personnel security requirements, including security roles and responsibilities for external providers;b. Require external providers to comply with personnel security policies and procedures established 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 and/or badges, or who have system privileges within [Assignment: organization-defined time period]; ande. Monitor provider compliance with personnel security requirements.	Functional	Equal	Third-Party Personnel Security	HRS-10	Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party cybersecurity and data protection roles and responsibilities.	10			PS-07	PS-07	PS-07	PS-07
PS-08	Personnel Sanctions	a. Employ a formal sanctions process for individuals failing to comply with established information security 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, identifying the individual sanctioned and the reason for the sanction.	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-08	PS-08	PS-08
RA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; andc. Review and update the current risk assessment:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5			RA-01	RA-01	RA-01	RA-01
RA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; andc. Review and update the current risk assessment:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	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	RA-01	RA-01
RA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, 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 official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; andc. Review and update the current risk assessment:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5			RA-01	RA-01	RA-01	RA-01
RA-02	Security Categorization	a. Categorize the system and information it processes, 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 security categorization decision.	Functional	Equal	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that: (1) Document the security categorization results (including supporting rationale) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner.	10			RA-02	RA-02	RA-02	RA-02
RA-03	Risk Assessment	a. Conduct a risk assessment, including:1. Identifying threats to and vulnerabilities in the system;2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;b. Integrate risk assessment results and 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; risk assessment report; [Assignment: organization-defined document]];d. Review risk assessment results [Assignment: organization-defined frequency];e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; andf. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.	Functional	Intersects With	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's cybersecurity and data protection policies and standards.	5			RA-03	RA-03	RA-03	RA-03

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
RA-03	Risk Assessment	a. Conduct a risk assessment, including:1. Identifying threats to and vulnerabilities in the system;2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;b. Integrate risk assessment results and 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; risk assessment report; [Assignment: organization-defined document]];d. Review risk assessment results [Assignment: organization-defined frequency];e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; andf. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5			RA-03	RA-03	RA-03	RA-03
RA-05	Vulnerability Monitoring and Scanning	a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:1. Enumerating platforms, software flaws, and 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 vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk;e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; andf. Employ vulnerability monitoring tools that include the capability to readily update the	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	RA-05	RA-05	RA-05
RA-05	Vulnerability Monitoring and Scanning	a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:1. Enumerating platforms, software flaws, and 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 vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk;e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; andf. Employ vulnerability monitoring tools that include the capability to readily update the	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5		RA-05	RA-05	RA-05	RA-05	RA-05
RA-05(01)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5		RA-05(01)	RA-05(01)	RA-05(01)	RA-05(01)
RA-05(02)	Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be	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(02)	RA-05(02)	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 identify the breadth and depth of coverage for vulnerability scanning that define the system components scanned and types of vulnerabilities that are	10					RA-05(03)	RA-05(03)
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 remediated non-compliant systems.	10						RA-05(04)
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(05)			RA-05(05)	RA-05(05)
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(06)	RA-05(06)
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(08)	RA-05(08)
RA-05(10)	Vulnerability Monitoring and Scanning | Correlate Scanning Information	Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors.	Functional	Equal	Correlate Scanning Information	VPM-06.9	Automated mechanisms exist to correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.	10						RA-05(10)
SA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, 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 official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; andc. Review and update the current system and services acquisition:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5			SA-01	SA-01	SA-01	SA-01
SA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, 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 official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; andc. Review and update the current system and services acquisition:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10			SA-01	SA-01	SA-01	SA-01

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
SA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, 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 official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; andc. Review and update the current system and services acquisition:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5			SA-01	SA-01	SA-01	SA-01
SA-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, 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 official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; andc. Review and update the current system and services acquisition:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5			SA-01	SA-01	SA-01	SA-01
SA-02	Allocation of Resources	a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;b. 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 line item for information security and privacy in organizational programming and budgeting documentation.	Functional	Equal	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	10			SA-02	SA-02	SA-02	SA-02
SA-03	System Development Life Cycle	a. Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information 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. Integrate the organizational information security and privacy risk management process into system development life cycle activities.	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	SA-03	SA-03
SA-03	System Development Life Cycle	a. Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information 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. Integrate the organizational information security and privacy risk management process into system development life cycle activities.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5			SA-03	SA-03	SA-03	SA-03
SA-04	Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:a. Security and privacy functional requirements;b. Strength of mechanism 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 protecting security and privacy documentation;g. Description of the system development environment and environment in which the system is intended to operate;h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; andi. Acceptance criteria.	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5						SA-04	SA-04
SA-04	Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:a. Security and privacy functional requirements;b. Strength of mechanism 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 protecting security and privacy documentation;g. Description of the system development environment and environment in which the system is intended to operate;h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; andi. Acceptance criteria.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5						SA-04	SA-04
SA-04	Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:a. Security and privacy functional requirements;b. Strength of mechanism 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 protecting security and privacy documentation;g. Description of the system development environment and environment in which the system is intended to operate;h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; andi. Acceptance criteria.	Functional	Intersects With	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	5						SA-04	SA-04
SA-04	Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:a. Security and privacy functional requirements;b. Strength of mechanism 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 protecting security and privacy documentation;g. Description of the system development environment and environment in which the system is intended to operate;h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; andi. Acceptance criteria.	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	5						SA-04	SA-04

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
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 security controls to be utilized within Technology Assets, Applications and/or Services (TAAS) in sufficient detail to permit analysis and testing of the controls.	5					SA-04(01)	SA-04(01)
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	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	5					SA-04(01)	SA-04(01)
SA-04(02)	Acquisition Process | Design and Implementation Information for Controls	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of detail].	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	5						SA-04(02)
SA-04(02)	Acquisition Process | Design and Implementation Information for Controls	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of	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)
SA-04(02)	Acquisition Process | Design and Implementation Information for Controls	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of detail].	Functional	Intersects With	Functional Properties	TDA-04.1	Mechanisms exist to require software developers to provide information describing the functional properties of the security controls to be utilized within Technology Assets, Applications and/or Services (TAAS) in sufficient detail to permit analysis and testing of the controls.	5						SA-04(02)
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 continuous monitoring of cybersecurity and data protection control effectiveness.	10						SA-04(08)
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 Secure Development Life Cycle (SDLC), the functions, ports, protocols and services intended for use.	10						SA-04(09)
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	Mechanisms exist to limit the use of commercially-provided Information Assurance (IA) and IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated or NSA-	5						SA-04(10)
SA-05	System Documentation	a. Obtain or develop administrator documentation for the system, system component, or system service that describes:1. Secure configuration, installation, and operation of the system, component, or service;2. Effective use and maintenance of security and privacy functions and mechanisms; and3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;b. Obtain or develop user documentation for the system, system component, or system service that describes:1. User-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 service in a more secure manner and protect individual privacy; and3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [Assignment: organization-defined actions] in response; andd. Distribute documentation to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5		SA-05	SA-05	SA-05	SA-05
SA-05	System Documentation	a. Obtain or develop administrator documentation for the system, system component, or system service that describes:1. Secure configuration, installation, and operation of the system, component, or service;2. Effective use and maintenance of security and privacy functions and mechanisms; and3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;b. Obtain or develop user documentation for the system, system component, or system service that describes:1. User-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 service in a more secure manner and protect individual privacy; and3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [Assignment: organization-defined actions] in response; andd. Distribute documentation to [Assignment: organization-defined personnel or roles].	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine cybersecurity and data protection control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).	5		SA-05	SA-05	SA-05	SA-05
SA-08	Security and Privacy Engineering Principles	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening	5					SA-08	SA-08
SA-08	Security and Privacy Engineering Principles	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications	5					SA-08	SA-08
SA-09	External System Services	a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [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 compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques].	Functional	Equal	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	10			SA-09	SA-09	SA-09	SA-09
SA-09(01)	External System Services | Risk Assessments and Organizational Approvals	a. Conduct an organizational assessment of risk prior 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 personnel or roles].	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 Assets, Applications and/or Services (TAAS).	10				SA-09(01)	SA-09(01)	SA-09(01)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
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	External Connectivity Requirements - Identification of Ports, Protocols & Services	TPM-04.2	Mechanisms exist to require External Service Providers (ESPs) to identify and document the business need for ports, protocols and other services it requires to operate its Technology Assets, Applications and/or Services	10				SA-09(02)	SA-09(02)	SA-09(02)
SA-09(04)	External System Services | Consistent Interests of Consumers and	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(04)
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	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5						SA-09(05)
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)
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	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.	5						SA-09(05)
SA-10	Developer Configuration Management	Require the developer of the system, system component, or system service to:a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation; disposal];b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];c. Implement only organization-approved changes to the system, component, or service;d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; ande. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].	Functional	Equal	Developer Configuration Management	TDA-14	Mechanisms exist to require system developers and integrators to perform configuration management during system design, development, implementation and operation.	10					SA-10	SA-10
SA-10(01)	Developer Configuration Management | Software and Firmware Integrity Verification	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 verification of software and firmware components.	10					SA-10(01)	SA-10(01)
SA-11	Developer Testing and Evaluation	Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:a. Develop and implement a plan for ongoing security 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 the assessment plan and the results of the testing and evaluation;d. Implement a verifiable flaw remediation process; ande. Correct flaws identified during testing and evaluation.	Functional	Equal	Cybersecurity & Data Protection Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity and data protection personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	10		SA-11		SA-11	SA-11	SA-11
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 analysis tools to identify and remediate common flaws and document the results of the analysis.	10		SA-11(01)			SA-11(01)	SA-11(01)
SA-11(02)	Developer Testing and Evaluation | Threat Modeling and Vulnerability Analyses	Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that:a. Uses the following contextual information: [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels];b. Employs the following tools and methods: [Assignment: organization-defined tools and methods];c. Conducts the modeling and analyses at the following level of rigor: [Assignment: organization-defined breadth and depth of modeling and analyses]; andd. Produces evidence that meets the following acceptance criteria: [Assignment: organization-defined acceptance criteria].	Functional	Intersects With	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5					SA-11(02)	SA-11(02)
SA-11(02)	Developer Testing and Evaluation | Threat Modeling and Vulnerability Analyses	Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that:a. Uses the following contextual information: [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels];b. Employs the following tools and methods: [Assignment: organization-defined tools and methods];c. Conducts the modeling and analyses at the following level of rigor: [Assignment: organization-defined breadth and depth of modeling and analyses]; andd. Produces evidence that meets the following acceptance criteria: [Assignment: organization-defined acceptance criteria].	Functional	Intersects With	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	5					SA-11(02)	SA-11(02)
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 analysis tools to identify and remediate common flaws and document the results of the analysis.	10					SA-11(08)	SA-11(08)
SA-12	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5					SA-12
SA-15	Development Process, Standards, and Tools	a. Require the developer of the system, system component, or system service to follow a documented development process that:1. Explicitly addresses security and privacy requirements;2. Identifies the standards and tools used in the development process;3. Documents the specific tool options and tool 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 [Assignment: organization-defined frequency] to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: [Assignment: organization-defined security and privacy requirements].	Functional	Equal	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	10						SA-15
SA-16	Developer-provided Training	Require the developer of the system, system component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: [Assignment: organization-defined training].	Functional	Equal	Developer-Provided Training	TDA-16	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to provide training on the correct use and operation of the Technology Asset, Application and/or Service (TAAS).	10						SA-16

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
SA-17	Developer Security and Privacy Architecture and Design	Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that:a. Is consistent with the organization's security and privacy architecture that is an integral part the organization's enterprise architecture;b. Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; andc. Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection.	Functional	Equal	Developer Architecture & Design	TDA-05	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a design specification and security architecture that: (1) Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; (2) Accurately and completely describes the required security functionality and the allocation of security controls among physical and logical components; and (3) Expresses how individual security functions, mechanisms and services work together to provide required security capabilities and a unified approach to protection.	10						SA-17
SC-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; andc. Review and update the current system and communications protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5			SC-01	SC-01	SC-01	SC-01
SC-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; andc. Review and update the current system and communications protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following	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	SC-01	SC-01
SC-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; andc. Review and update the current system and communications protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10			SC-01	SC-01	SC-01	SC-01
SC-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; andc. Review and update the current system and communications protection:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5			SC-01	SC-01	SC-01	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		SC-02		SC-02	SC-02	SC-02
SC-03	Security Function Isolation	Isolate security functions from nonsecurity functions.	Functional	Intersects With	Restrict Access To Security Functions	END-16	Mechanisms exist to ensure security functions are restricted to authorized individuals and enforce least privilege control requirements for necessary job functions.	5						SC-03
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
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		SC-04	SC-04	SC-04
SC-05	Denial-of-service Protection	a. [Selection (one): Protect against; Limit] the effects of 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-service event].	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5			SC-05	SC-05	SC-05	SC-05
SC-05	Denial-of-service Protection	a. [Selection (one): Protect against; Limit] the effects of 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-service event].	Functional	Intersects With	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	5			SC-05	SC-05	SC-05	SC-05
SC-05	Denial-of-service Protection	a. [Selection (one): Protect against; Limit] the effects of 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-service event].	Functional	Intersects With	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	5			SC-05	SC-05	SC-05	SC-05

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
SC-05	Denial-of-service Protection	a. [Selection (one): Protect against; Limit] the effects of 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-service event].	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	SC-05	SC-05
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 susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5					SC-06	SC-06
SC-07	Boundary Protection	a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;b. Implement subnetworks for publicly accessible system components that are [Selection (one): physically; logically] separated from internal organizational networks; andc. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.	Functional	Intersects With	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	SC-07	SC-07	SC-07
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 and/or Services (TAAS).	10		SC-07(03)			SC-07(03)	SC-07(03)
SC-07(04)	Boundary Protection | External Telecommunications Services	a. Implement a managed interface for each external telecommunication service;b. Establish a traffic flow policy for each managed interface;c. Protect the confidentiality and integrity of the information being transmitted across each interface;d. Document each exception to the traffic flow policy with a supporting 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 unauthorized exchange of control plane traffic with external networks;g. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; andh. Filter unauthorized control plane traffic from external networks.	Functional	Intersects With	External Telecommunications Services	NET-03.2	Mechanisms exist to maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface.	5					SC-07(04)	SC-07(04)
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	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5				SC-07(05)	SC-07(05)	SC-07(05)
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	10				SC-07(07)	SC-07(07)	SC-07(07)
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	5					SC-07(08)	SC-07(08)
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	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5					SC-07(08)	SC-07(08)
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						SC-07(10)
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(10)
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(12)	SC-07(12)	SC-07(12)
SC-07(13)	Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components	Isolate [Assignment: organization-defined information security tools, mechanisms, and support components] from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.	Functional	Intersects With	Security Management Subnets	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the	5				SC-07(13)	SC-07(13)	SC-07(13)
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 cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications	5					SC-07(18)	SC-07(18)
SC-07(20)	Boundary Protection | Dynamic Isolation and Segregation	Provide the capability to dynamically isolate [Assignment: organization-defined system components] from other system components.	Functional	Equal	Dynamic Isolation & Segregation (Sandboxing)	NET-03.6	Automated mechanisms exist to dynamically isolate (e.g., sandbox) untrusted components during runtime, where the component is isolated in a fault-contained environment but it can still collaborate with the application.	10						SC-07(20)
SC-07(21)	Boundary Protection | Isolation of System Components	Employ boundary protection mechanisms to isolate [Assignment: organization-defined system components] supporting [Assignment: organization-defined missions and/or business functions].	Functional	Equal	Isolation of System Components	NET-03.7	Mechanisms exist to employ boundary protections to isolate Technology Assets, Applications and/or Services (TAAS) that support critical missions and/or business functions.	10						SC-07(21)
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	SC-08	SC-08
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	SC-08	SC-08
SC-08(01)	Transmission Confidentiality and Integrity | Cryptographic	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)	SC-08(01)
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)	SC-08(01)
SC-08(01)	Transmission Confidentiality and Integrity | Cryptographic	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(01)	SC-08(01)
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-10	SC-10	SC-10
SC-12	Cryptographic Key Establishment and Management	Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].	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	SC-12	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(01)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
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	Mechanisms exist to facilitate the production and management of symmetric cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key management technology and processes.	10					SC-12(02)	SC-12(02)
SC-12(03)	Cryptographic Key Establishment and Management | Asymmetric Keys	Produce, control, and distribute asymmetric cryptographic keys using [Selection (one): NSA-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 protect the user's private key; certificates issued in accordance with organization-defined requirements].	Functional	Equal	Asymmetric Keys	CRY-09.2	Mechanisms exist to facilitate the production and management of asymmetric cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key management technology and processes that protect the user's private key.	10					SC-12(03)	SC-12(03)
SC-13	Cryptographic Protection	a. Determine the [Assignment: organization-defined 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 use].	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	SC-13	SC-13	SC-13
SC-13	Cryptographic Protection	a. Determine the [Assignment: organization-defined 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 use].	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	SC-13	SC-13	SC-13
SC-13	Cryptographic Protection	a. Determine the [Assignment: organization-defined 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 use].	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	SC-13	SC-13	SC-13
SC-15	Collaborative Computing Devices and Applications	a. Prohibit remote activation of collaborative 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 physically present at the devices.	Functional	Intersects With	Collaborative Computing Devices	END-14	Mechanisms exist to unplug or prohibit the remote activation of collaborative computing devices with the following exceptions: (1) Networked whiteboards; (2) Video teleconference cameras; and	5						SC-15
SC-17	Public Key Infrastructure Certificates	a. Issue public key certificates under an [Assignment: 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 organization.	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-17	SC-17	SC-17
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	SC-18
SC-19	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5				SC-19	SC-19
SC-20	Secure Name/address Resolution Service (authoritative Source)	a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns 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 chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.	Functional	Intersects With	Domain Name Service (DNS) Resolution	NET-10	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5			SC-20	SC-20	SC-20	SC-20
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	Mechanisms exist to perform data origin authentication and data integrity verification on the Domain Name Service (DNS) resolution responses received from authoritative sources when requested by client systems.	10		SC-21	SC-21	SC-21	SC-21	SC-21
SC-22	Architecture and Provisioning for Name/address Resolution Service	Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.	Functional	Equal	Architecture & Provisioning for Name / Address Resolution Service	NET-10.1	Mechanisms exist to ensure systems that collectively provide Domain Name Service (DNS) resolution service are fault-tolerant and implement internal/external role separation.	10			SC-22	SC-22	SC-22	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	SC-23
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	10						SC-23(01)
SC-24	Fail in Known State	Fail to a [Assignment: organization-defined known system state] for the following failures on the indicated components while preserving [Assignment: organization-defined system state information] in failure: [Assignment: list of organization-defined types of system failures on organization-defined system components].	Functional	Intersects With	Fail Secure	SEA-07.2	Mechanisms exist to enable systems to fail to an organization-defined known-state for types of failures, preserving system state information in failure.	5						SC-24
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		SC-28	SC-28	SC-28
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	SC-28	SC-28
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)	SC-28(01)
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)	SC-28(01)
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)	SC-28(01)
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(01)	SC-28(01)
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	SC-39	SC-39
SI-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and information integrity policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; andc. Review and update the current system and information integrity:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5			SI-01	SI-01	SI-01	SI-01

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
SI-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and information integrity policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; andc. Review and update the current system and information integrity:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10			SI-01	SI-01	SI-01	SI-01
SI-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and information integrity policy that:a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; andb. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; andc. Review and update the current system and information integrity:1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5			SI-01	SI-01	SI-01	SI-01
SI-02	Flaw Remediation	a. Identify, report, and correct system flaws;b. Test software and firmware updates related to flaw 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 updates; andd. Incorporate flaw remediation into the organizational configuration management process.	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	SI-02	SI-02	SI-02
SI-02	Flaw Remediation	a. Identify, report, and correct system flaws;b. Test software and firmware updates related to flaw 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 updates; andd. Incorporate flaw remediation into the organizational configuration management process.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		SI-02	SI-02	SI-02	SI-02	SI-02
SI-02	Flaw Remediation	a. Identify, report, and correct system flaws;b. Test software and firmware updates related to flaw 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 updates; andd. Incorporate flaw remediation into the organizational configuration management process.	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	SI-02	SI-02	SI-02
SI-02(01)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5					SI-02(01)
SI-02(02)	Flaw Remediation | Automated Flaw Remediation Status	Determine if system components have applicable security-relevant software and firmware updates installed using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency].	Functional	Intersects With	Automated Remediation Status	VPM-05.2	Automated mechanisms exist to determine the state of system components with regard to flaw remediation.	5		SI-02(02)			SI-02(02)	SI-02(02)
SI-02(03)	Flaw Remediation | Time to Remediate Flaws and Benchmarks for	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(03)	SI-02(03)
SI-03	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;c. Configure malicious code protection mechanisms to:1. Perform periodic scans of the system [Assignment: 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 with organizational policy; and2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; andd. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		SI-03	SI-03	SI-03	SI-03	SI-03
SI-03	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;c. Configure malicious code protection mechanisms to:1. Perform periodic scans of the system [Assignment: 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 with organizational policy; and2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; andd. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	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	SI-03	SI-03	SI-03
SI-03	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;c. Configure malicious code protection mechanisms to:1. Perform periodic scans of the system [Assignment: 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 with organizational policy; and2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; andd. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	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	SI-03	SI-03	SI-03

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
SI-03	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;c. Configure malicious code protection mechanisms to:1. Perform periodic scans of the system [Assignment: 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 with organizational policy; and2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; andd. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	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	SI-03	SI-03	SI-03
SI-03	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;c. Configure malicious code protection mechanisms to:1. Perform periodic scans of the system [Assignment: 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 with organizational policy; and2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; andd. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5		SI-03	SI-03	SI-03	SI-03	SI-03
SI-03	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;c. Configure malicious code protection mechanisms to:1. Perform periodic scans of the system [Assignment: 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 with organizational policy; and2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; andd. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	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	SI-03	SI-03	SI-03
SI-03	Malicious Code Protection	a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;c. Configure malicious code protection mechanisms to:1. Perform periodic scans of the system [Assignment: 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 with organizational policy; and2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; andd. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5		SI-03	SI-03	SI-03	SI-03	SI-03
SI-03(01)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5				SI-03(01)	SI-03(01)
SI-03(02)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5				SI-03(02)	SI-03(02)
SI-03(07)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5				SI-03(07)	SI-03(07)
SI-04	System Monitoring	a. Monitor the system to detect:1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and2. Unauthorized local, network, and remote connections;b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];c. Invoke internal monitoring capabilities or 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 and anomalies;e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;f. Obtain legal opinion regarding system monitoring activities; andg. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment:	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5		SI-04	SI-04	SI-04	SI-04	SI-04
SI-04	System Monitoring	a. Monitor the system to detect:1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and2. Unauthorized local, network, and remote connections;b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];c. Invoke internal monitoring capabilities or 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 and anomalies;e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;f. Obtain legal opinion regarding system monitoring activities; andg. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment:	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.	5		SI-04	SI-04	SI-04	SI-04	SI-04

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
SI-04	System Monitoring	a. Monitor the system to detect:1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and2. Unauthorized local, network, and remote connections;b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];c. Invoke internal monitoring capabilities or 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 and anomalies;e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;f. Obtain legal opinion regarding system monitoring activities; andg. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment:	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5		SI-04	SI-04	SI-04	SI-04	SI-04
SI-04	System Monitoring	a. Monitor the system to detect:1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and2. Unauthorized local, network, and remote connections;b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];c. Invoke internal monitoring capabilities or 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 and anomalies;e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;f. Obtain legal opinion regarding system monitoring activities; andg. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment:	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5		SI-04	SI-04	SI-04	SI-04	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	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	10					SI-04(01)	SI-04(01)
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(02)	SI-04(02)
SI-04(04)	System Monitoring | Inbound and Outbound Communications Traffic	a. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;b. Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].	Functional	Equal	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	10		SI-04(04)			SI-04(04)	SI-04(04)
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 and supply chain activities to achieve integrated	10					SI-04(05)	SI-04(05)
SI-04(11)	System Monitoring | Analyze Communications Traffic Anomalies	Analyze outbound communications traffic at the external interfaces to the system and selected [Assignment: organization-defined interior points within the system] to discover anomalies.	Functional	Equal	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	10						SI-04(11)
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 Intrusion Detection System (WIDS)	MON-01.5	Mechanisms exist to utilize Wireless Intrusion Detection / Protection Systems (WIDS / WIPS) to identify rogue wireless devices and to detect attack attempts via wireless networks.	5					SI-04(14)	SI-04(14)
SI-04(16)	System Monitoring | Correlate Monitoring Information	Correlate information from monitoring tools and mechanisms employed throughout the system.	Functional	Equal	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	10					SI-04(16)	SI-04(16)
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)
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(18)
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(19)
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(20)
SI-04(22)	System Monitoring | Unauthorized Network Services	a. Detect network services that have not been authorized or approved by [Assignment: organization-defined authorization or approval processes]; andb. [Selection (one or more): Audit; Alert [Assignment: organization-defined personnel or roles]] when detected.	Functional	Equal	Unauthorized Network Services	MON-11.2	Automated mechanisms exist to detect unauthorized network services and alert incident response personnel.	10						SI-04(22)
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	Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS) to actively alert on or block unwanted activities and send logs to a Security Incident Event Manager (SIEM), or similar automated tool, to maintain situational	10					SI-04(23)	SI-04(23)
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)
SI-04(24)	System Monitoring | Indicators of Compromise	Discover, collect, and distribute to [Assignment: organization-defined personnel or roles], indicators of compromise provided by [Assignment: organization-defined sources].	Functional	Intersects With	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets, Applications and/or Services (TAAS) to generate alerts for unauthorized	5						SI-04(24)
SI-05	Security Alerts, Advisories, and Directives	a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;b. Generate internal security alerts, advisories, and 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: organization-defined external organizations]]; andd. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5			SI-05	SI-05	SI-05	SI-05

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
SI-05	Security Alerts, Advisories, and Directives	a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;b. Generate internal security alerts, advisories, and 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: organization-defined external organizations]]; andd. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.	Functional	Intersects With	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5			SI-05	SI-05	SI-05	SI-05
SI-05	Security Alerts, Advisories, and Directives	a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;b. Generate internal security alerts, advisories, and 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: organization-defined external organizations]]; andd. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5			SI-05	SI-05	SI-05	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 Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating	5						SI-05(01)
SI-06	Security and Privacy Function Verification	a. Verify the correct operation of [Assignment: organization-defined security and privacy functions];b. Perform the verification of the functions specified in SI-06a [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]];c. Alert [Assignment: organization-defined personnel or roles] to failed security and privacy verification tests; andd. [Selection (one or more): Shut the system down; Restart the system; [Assignment: organization-defined alternative action(s)]] when anomalies are	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of cybersecurity and/or data privacy controls following implemented changes to ensure applicable controls operate as designed.	5						SI-06	SI-06
SI-07	Software, Firmware, and Information Integrity	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; andb. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	5		SI-07		SI-07	SI-07	SI-07
SI-07	Software, Firmware, and Information Integrity	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; andb. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5		SI-07		SI-07	SI-07	SI-07
SI-07	Software, Firmware, and Information Integrity	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; andb. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5		SI-07		SI-07	SI-07	SI-07
SI-07(01)	Software, Firmware, and Information Integrity | Integrity Checks	Perform an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]].	Functional	Equal	Integrity Checks	END-06.1	Mechanisms exist to validate configurations through integrity checking of software and firmware.	10					SI-07(01)	SI-07(01)
SI-07(02)	Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations	Employ automated tools that provide notification to [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification.	Functional	Equal	Automated Notifications of Integrity Violations	END-06.3	Automated mechanisms exist to alert incident response personnel upon discovering discrepancies during integrity verification.	10						SI-07(02)
SI-07(05)	Software, Firmware, and Information Integrity | Automated Response to Integrity Violations	Automatically [Selection (one or more): shut the system down; restart the system; implement [Assignment: organization-defined controls]] when integrity violations are discovered.	Functional	Equal	Automated Response to Integrity Violations	END-06.4	Automated mechanisms exist to implement remediation actions when integrity violations are discovered.	10						SI-07(05)
SI-07(07)	Software, Firmware, and Information Integrity | Integration of Detection and Response	Incorporate the detection of the following unauthorized changes into the organizational incident response capability: [Assignment: organization-defined security-relevant changes to the system].	Functional	Equal	Endpoint Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.	10		SI-07(07)			SI-07(07)	SI-07(07)
SI-07(14)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5					SI-07(14)
SI-08	Spam Protection	a. Employ spam protection mechanisms at system 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 procedures.	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	SI-08	SI-08
SI-08(01)	N/A	Withdrawn	Functional	not related to	N/A	N/A	N/A	0	Withdrawn in NIST SP 800-53 R5				SI-08(01)	SI-08(01)
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	Mechanisms exist to automatically update anti-phishing and spam protection technologies when new releases are available in accordance with configuration and change management practices.	10					SI-08(02)	SI-08(02)
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	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5				SI-10	SI-10	SI-10
SI-10	Information Input Validation	Check the validity of the following information inputs: [Assignment: organization-defined information inputs to the	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5				SI-10	SI-10	SI-10
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	Mechanisms exist to handle error conditions by: (1) Identifying potentially security-relevant error conditions; (2) Generating error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited; and (3) Revealing error messages only to authorized personnel.	10				SI-11	SI-11	SI-11
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	SI-12	SI-12	SI-12
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 Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5			SI-12	SI-12	SI-12	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 Relationshi	Notes	Core	Low	Low+	Moderate	High (FedRAMP)
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-16	SI-16	SI-16	SI-16