

**NIST IR 8477-Based Set Theory Relationship Mapping .STRM**

**Reference Document:** Secure Controls Framework (SCF) version 2026.1  
<https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/>

**Focal Document:**  
**Focal Document URL:**  
**Published STRM URL:**

**Centers for Medicare & Medicaid Services MARS-E Document Suite, Version 2.0**  
<https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/3-MARS-E-v2-0-Catalog-of-Security-and-Privacy-Controls-1102015.pdf>  
<https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-cms-mars-e-v2-0.pdf>

| FDE #         | FDE Name  | Focal Document Element (FDE) Description  | STRM Rationale | STRM Relationship | SCF Control   | SCF #    | Secure Controls Framework (SCF) Control Description   | Strength of Relationship | Notes                     |
|---------------|---|---|----------------|-------------------|---|----------|---|--------------------------|---------------------------|
| 1             | Security Controls Detail and Control Implementation Description | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A   | 0                        | No applicable SCF control |
| 1.1           | Access Control (AC)   | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A   | 0                        | No applicable SCF control |
| AC-1          | Access Control (AC)   | The organization develops, documents, disseminates to applicable personnel, and reviews and updates (as necessary) within every three hundred sixty-five (365) days:  | Functional     | Intersects With   | Publishing Security, Compliance & Resilience Documentation            | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.  | 5                        |                           |
| AC-1          | Access Control (AC)   | The organization develops, documents, disseminates to applicable personnel, and reviews and updates (as necessary) within every three hundred sixty-five (365) days:  | Functional     | Intersects With   | Periodic Review & Update of Security, Compliance & Resilience Program | GOV-03   | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. | 5                        |                           |
| AC-1          | Access Control (AC)   | The organization develops, documents, disseminates to applicable personnel, and reviews and updates (as necessary) within every three hundred sixty-five (365) days:  | Functional     | Subset Of         | Identity & Access Management (IAM)                                    | IAC-01   | Mechanisms exist to facilitate the implementation of identification and access management controls.   | 10                       |                           |
| AC-1.a        | Access Control Policy and Procedures                            | An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and   | Functional     | Subset Of         | Publishing Security, Compliance & Resilience Documentation            | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.  | 10                       |                           |
| AC-1.b        | Access Control Policy and Procedures                            | Procedures to facilitate that implementation of the access control policy and associated access controls.   | Functional     | Subset Of         | Standardized Operating Procedures (SOP)                               | OPS-01.1 | Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.   | 10                       |                           |
| AC-2          | Account Management  | The organization:   | Functional     | Intersects With   | Termination of Employment   | IAC-07.2 | Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.   | 5                        |                           |
| AC-2          | Account Management  | The organization:   | Functional     | Intersects With   | Account Management  | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.   | 5                        |                           |
| AC-2          | Account Management  | The organization:   | Functional     | Intersects With   | Input Data Validation   | TDA-18   | Mechanisms exist to check the validity of information inputs.   | 5                        |                           |
| AC-2          | Account Management  | The organization:   | Functional     | Intersects With   | Safeguarding Data Over Open Networks                                  | NET-12   | Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.  | 5                        |                           |
| AC-2.a        | Account Management  | Identifies and selects the following types of information system (IS) accounts to support organizational mission/business functions: individual, group, system, application, guest/anonymous, emergency, and temporary;   | Functional     | Subset Of         | Account Management  | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.   | 10                       |                           |
| AC-2.b        | Account Management  | Assigns account managers for IS accounts;   | Functional     | Subset Of         | Account Management  | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.   | 10                       |                           |
| AC-2.c        | Account Management  | Establishes conditions for group and role membership;   | Functional     | Subset Of         | Account Management  | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.   | 10                       |                           |
| AC-2.d        | Account Management  | Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges and other attributes (as required) for each account);  | Functional     | Subset Of         | Account Management  | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.   | 10                       |                           |
| AC-2.e        | Account Management  | Requires approvals by defined personnel or roles (defined in the applicable security plan) for requests to create IS accounts;  | Functional     | Subset Of         | Account Management  | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.   | 10                       |                           |
| AC-2.f        | Account Management  | Establishes organizational standards and procedures for creating, enabling, modifying, disabling, and removing IS accounts for each account type. These procedures include the following activities:  | Functional     | Subset Of         | Account Management  | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.   | 10                       |                           |
| AC-2.f.1      | Account Management  | Authorizing access to the IS based on:  | Functional     | Subset Of         | Account Management  | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.   | 10                       |                           |
| AC-2.f.1(i)   | Account Management  | A valid access authorization;   | Functional     | Subset Of         | Account Management  | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.   | 10                       |                           |
| AC-2.f.1(ii)  | Account Management  | Intended system usage; and  | Functional     | Subset Of         | Account Management  | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.   | 10                       |                           |
| AC-2.f.1(iii) | Account Management  | Other attributes as required by the organization or associated mission/business functions;  | Functional     | Subset Of         | Account Management  | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.   | 10                       |                           |
| AC-2.f.2      | Account Management  | Monitoring the use of information system accounts;  | Functional     | Subset Of         | Account Management  | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.   | 10                       |                           |
| AC-2.f.3      | Account Management  | Notifying account managers:   | Functional     | Subset Of         | Account Management  | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.   | 10                       |                           |
| AC-2.f.3(i)   | Account Management  | When accounts are no longer required;   | Functional     | Subset Of         | Account Management  | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.   | 10                       |                           |
| AC-2.f.3(ii)  | Account Management  | When users are terminated or transferred; and   | Functional     | Subset Of         | Account Management  | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.   | 10                       |                           |
| AC-2.f.3(iii) | Account Management  | When individual information system usage or need-to-know changes;   | Functional     | Subset Of         | Account Management  | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.   | 10                       |                           |
| AC-2.g        | Account Management  | Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.   | Functional     | Subset Of         | Account Management  | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.   | 10                       |                           |
| AC-2.h.1      | Account Management  | Review information system accounts for compliance with account management requirements within every one hundred eighty (180) days, and require annual certification of all accounts within every three hundred sixty-five (365) days.   | Functional     | Subset Of         | Account Management  | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.   | 10                       |                           |
| AC-2.h.2      | Account Management  | Remove or disable default user accounts. Rename active default accounts.  | Functional     | Subset Of         | Account Management  | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.   | 10                       |                           |
| AC-2.h.3      | Account Management  | Implement centralized control of user access administrator functions.   | 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                        |                           |
| AC-2.h.3      | Account Management  | Implement centralized control of user access administrator functions.   | 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-2.h.4      | Account Management  | Regulate the access provided to contractors and define security requirements for contractors.   | Functional     | Subset Of         | Account Management  | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.   | 10                       |                           |
| AC-2(i)       | Automated Information System Account Management                 | The organization employs automated mechanisms to support the management of information system accounts.   | 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-2(j)       | Removal of Temporary/Emergency Accounts                         | The information system automatically disables emergency accounts within twenty-four (24) hours and temporary accounts with a fixed duration not to exceed three hundred sixty-five (365) days.  | Functional     | Subset Of         | Removal of Temporary / Emergency Accounts                             | IAC-15.2 | Automated mechanisms exist to disable or remove temporary and emergency accounts after an organization-defined time period for each type of account.  | 10                       |                           |
| AC-2(k)       | Disable Inactive Accounts                                       | N/A   | Functional     | Subset Of         | Disable Inactive Accounts   | IAC-15.3 | Automated mechanisms exist to disable inactive accounts after an organization-defined time period.  | 10                       |                           |
| AC-2(l).a     | Disable Inactive Accounts                                       | The information system automatically disables inactive accounts within sixty (60) days; and   | Functional     | Subset Of         | Disable Inactive Accounts   | IAC-15.3 | Automated mechanisms exist to disable inactive accounts after an organization-defined time period.  | 10                       |                           |
| AC-2(l).b     | Disable Inactive Accounts                                       | The organization defines the time period for non-user accounts (e.g., accounts associated with devices such as service accounts).   | Functional     | Subset Of         | Disable Inactive Accounts   | IAC-15.3 | Automated mechanisms exist to disable inactive accounts after an organization-defined time period.  | 10                       |                           |
| AC-2(l)       | Automated Audit Actions   | The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies defined personnel or roles defined in the applicable security plan.  | Functional     | Subset Of         | 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(m)       | Role-Based Schemes  | The organization:   | Functional     | Subset Of         | Role-Based Access Control (RBAC)                                      | IAC-08   | Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.                                | 10                       |                           |
| AC-2(n).a     | Role-Based Schemes  | Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;  | Functional     | Subset Of         | Role-Based Access Control (RBAC)                                      | IAC-08   | Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.                                | 10                       |                           |
| AC-2(n).b     | Role-Based Schemes  | Establishes and administers application-specific privileged user accounts in accordance with a role-based access scheme that allows access based on user responsibilities associated with application use;  | Functional     | Subset Of         | Role-Based Access Control (RBAC)                                      | IAC-08   | Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.                                | 10                       |                           |
| AC-2(n).c     | Role-Based Schemes  | Monitors privileged role assignments as well as application-specific privileged role assignments; and   | Functional     | Subset Of         | Role-Based Access Control (RBAC)                                      | IAC-08   | Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.                                | 10                       |                           |
| AC-2(n).d     | Role-Based Schemes  | Inspects administrator groups, root accounts, and other system-related accounts on demand, and at least once every fourteen (14) days to ensure that unauthorized accounts have not been created. Privileged user roles associated with applications should be inspected every thirty (30) days.  | Functional     | Subset Of         | Role-Based Access Control (RBAC)                                      | IAC-08   | Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.                                | 10                       |                           |
| AC-3          | Access Enforcement  | The information system enforces 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-3          | Access Enforcement  | The information system enforces 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-3          | Access Enforcement  | The information system enforces 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-3.h.1      | Access Enforcement  | If encryption is used as an access control mechanism, it must meet FIPS 140-2 compliant encryption standards (see SC-13).   | Functional     | Subset Of         | Secure Baseline Configurations  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.                                     | 10                       |                           |
| AC-3.h.2      | Access Enforcement  | Configure operating system controls to disable public "read" and "write" access to files, objects, and directories that may directly impact system functionality and/or performance, or that contain sensitive information.   | Functional     | Subset Of         | Secure Baseline Configurations  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.                                     | 10                       |                           |
| AC-3.h.3      | Access Enforcement  | Data stored in the information system must be protected with system access controls.  | Functional     | Subset Of         | Secure Baseline Configurations  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.                                     | 10                       |                           |
| AC-3.h.4      | Access Enforcement  | When contracting with external service providers, Personally Identifiable Information (PII), as well as software and services that receive, process, store, or transmit PII must be isolated within the service provider environment to the maximum extent possible so that other service provider customers sharing physical or virtual space cannot gain access to such data or applications. | Functional     | Subset Of         | Secure Baseline Configurations  | CFG-02   | Mechanisms exist to develop, document, and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.                                    | 10                       |                           |
| AC-3(i)       | Access Enforcement - Controlled Release                         | The information system does not release information outside of the established system boundary unless:  | Functional     | Subset Of         | Controlled Release  | DCH-03.3 | Automated mechanisms exist to validate cybersecurity and data protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  | 10                       |                           |
| AC-3(i).a     | Access Enforcement - Controlled Release                         | The receiving organization information system or system component provides organization security safeguards; and  | Functional     | Subset Of         | Controlled Release  | DCH-03.3 | Automated mechanisms exist to validate cybersecurity and data protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  | 10                       |                           |

| FDE #       | FDE Name  | Focal Document Element (FDE) Description   | STRM Rationale | STRM Relationship | SCF Control   | SCF #    | Secure Controls Framework (SCF) Control Description   | Strength of Relationship | Notes |
|-------------|---|--|----------------|-------------------|---|----------|---|--------------------------|-------|
| AC-3(9).b   | Access Enforcement - Controlled Release                           | The organization defined safeguards consistent with 45 CFR §155.260 Paragraph (b) (2) are used to validate the appropriateness of the information designated for release.  | Functional     | Subset Of         | Controlled Release  | DCH-03.3 | Automated mechanisms exist to validate cybersecurity and data protection attributes prior to releasing information to external Technology Assets, Applications and/or Services (TAAS).  | 10                       |       |
| AC-4        | Information Flow Enforcement                                      | The information system enforces approved authorizations for controlling the flow of information between the system and between interconnected systems in accordance with applicable policy.  | Functional     | Subset Of         | Data Flow Enforcement - Access Control Lists (ACLs)               | NET-04   | Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.  | 10                       |       |
| AC-5        | Separation of Duties  | The organization:<br>Maintain a limited group of administrators with access based upon the users' roles and responsibilities.  | Functional     | Intersects With   | Input Data Validation   | TDA-18   | Mechanisms exist to check the validity of information inputs.   | 5                        |       |
| AC-5        | Separation of Duties  | The organization:<br>Maintain a limited group of administrators with access based upon the users' roles and responsibilities.  | 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-5        | Separation of Duties  | The organization:<br>Maintain a limited group of administrators with access based upon the users' roles and responsibilities.  | Functional     | Intersects With   | Safeguarding Data Over Open Networks                              | NET-12   | Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulate data during transmission over open, public networks.   | 5                        |       |
| AC-5.a      | Separation of Duties  | Separates duties of individuals as necessary to prevent malevolent activity without collusion.   | Functional     | Subset Of         | 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-5.b      | Separation of Duties  | Documents separation of duties; and  | Functional     | Subset Of         | Separation of Duties (SoD)  | HRS-11   | Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.  | 10                       |       |
| AC-5.c      | Separation of Duties  | Defines information system access authorizations to support separation of duties.  | Functional     | Subset Of         | Separation of Duties (SoD)  | HRS-11   | Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.  | 10                       |       |
| AC-5-1.1    | Separation of Duties  | Ensure that audit functions are not performed by security personnel responsible for administering access control.  | Functional     | Subset Of         | Separation of Duties (SoD)  | HRS-11   | Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.  | 10                       |       |
| AC-5-1.2    | Separation of Duties  | Ensure that critical mission functions and information system support functions are divided among separate individuals.  | Functional     | Subset Of         | Separation of Duties (SoD)  | HRS-11   | Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.  | 10                       |       |
| AC-5-1.3    | Separation of Duties  | Ensure that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups.   | Functional     | Subset Of         | Separation of Duties (SoD)  | HRS-11   | Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.  | 10                       |       |
| AC-5-1.4    | Separation of Duties  | Ensure that an independent entity, not the Business Owner, System Developer(s)/Maintainer(s), or System Administrator(s) responsible for the information system, conducts information security testing of the information system.  | Functional     | Subset Of         | Separation of Duties (SoD)  | HRS-11   | Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.  | 10                       |       |
| AC-5-1.5    | Separation of Duties  | Ensure that an independent entity, not the Business Owner, System Developer(s)/Maintainer(s), or System Administrator(s) responsible for the information system, conducts information security testing of the information system.  | Functional     | Subset Of         | Separation of Duties (SoD)  | HRS-11   | Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.  | 10                       |       |
| AC-6        | Least Privilege   | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with the organization's missions and business functions.<br>This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information.  | 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-6        | Least Privilege   | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with the organization's missions and business functions.<br>This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information.  | 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-6-1.1    | Least Privilege   | Disable all file system access not explicitly required for system, application, and administrator functionality.   | Functional     | Subset Of         | 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.                             | 10                       |       |
| AC-6-1.2    | Least Privilege   | Contractors must be provided with minimal system and physical access, and must agree to and support the CMS security requirements. The contractor selection process must assess the contractor's ability to adhere to and support the organization's security policy.  | Functional     | Subset Of         | 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.                             | 10                       |       |
| AC-6-1.3    | Least Privilege   | Restrict the use of database management utilities to only authorized database administrators. Prevent users from accessing database data files at the logical data view, field, or field-value level. Implement table-level access control.  | Functional     | Subset Of         | 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.                             | 10                       |       |
| AC-6-1.4    | Least Privilege   | Ensure that only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties.   | Functional     | Subset Of         | 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.                             | 10                       |       |
| AC-6-1.5    | Least Privilege   | Disable all system and removable media boot access unless it is explicitly authorized by the CIO for compelling operational needs. System and removable media boot access is authorized, boot access is password protected.  | Functional     | Subset Of         | Secure Baseline Configurations                                    | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.               | 10                       |       |
| AC-6(1)     | Authorize Access to Security Functions                            | At a minimum, the organization explicitly authorizes access to the following list of security functions (deployed in hardware, software, and firmware) and security-relevant information for all system components:  | Functional     | Subset Of         | Authorize Access to Security Functions                            | IAC-21.1 | Mechanisms exist to limit access to security functions to explicitly-authorized privileged users.   | 10                       |       |
| AC-6(1).a   | Authorize Access to Security Functions                            | Setting/modifying audit logs and auditing behavior;  | Functional     | Subset Of         | Authorize Access to Security Functions                            | IAC-21.1 | Mechanisms exist to limit access to security functions to explicitly-authorized privileged users.   | 10                       |       |
| AC-6(1).b   | Authorize Access to Security Functions                            | Setting/modifying boundary protection system rules;  | Functional     | Subset Of         | Authorize Access to Security Functions                            | IAC-21.1 | Mechanisms exist to limit access to security functions to explicitly-authorized privileged users.   | 10                       |       |
| AC-6(1).c   | Authorize Access to Security Functions                            | Configuring/modifying access authorizations (i.e., permissions, privileges);   | Functional     | Subset Of         | Authorize Access to Security Functions                            | IAC-21.1 | Mechanisms exist to limit access to security functions to explicitly-authorized privileged users.   | 10                       |       |
| AC-6(1).d   | Authorize Access to Security Functions                            | Setting/modifying authentication parameters; and   | Functional     | Subset Of         | Authorize Access to Security Functions                            | IAC-21.1 | Mechanisms exist to limit access to security functions to explicitly-authorized privileged users.   | 10                       |       |
| AC-6(1).e   | Authorize Access to Security Functions                            | Setting/modifying system configurations and parameters.  | Functional     | Subset Of         | Authorize Access to Security Functions                            | IAC-21.1 | Mechanisms exist to limit access to security functions to explicitly-authorized privileged users.   | 10                       |       |
| AC-6(1)-1.1 | Authorize Access to Security Functions                            | The System Owner explicitly authorizes access to organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information for authorized personnel, including, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.  | Functional     | Subset Of         | Authorize Access to Security Functions                            | IAC-21.1 | Mechanisms exist to limit access to security functions to explicitly-authorized privileged users.   | 10                       |       |
| AC-6(2)     | Non-Privileged Access for Non-Security Functions                  | At a minimum, the organization requires that users of information system accounts, or roles, with access to the following list of security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audit any use of privileged accounts, or roles, for such functions:  | Functional     | Subset Of         | Non-Privileged Access for Non-Security Functions                  | IAC-21.2 | Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.  | 10                       |       |
| AC-6(2).a   | Non-Privileged Access for Non-Security Functions                  | Setting/modifying audit logs and auditing behavior;  | Functional     | Subset Of         | Non-Privileged Access for Non-Security Functions                  | IAC-21.2 | Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.  | 10                       |       |
| AC-6(2).b   | Non-Privileged Access for Non-Security Functions                  | Setting/modifying boundary protection system rules;  | Functional     | Subset Of         | Non-Privileged Access for Non-Security Functions                  | IAC-21.2 | Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.  | 10                       |       |
| AC-6(2).c   | Non-Privileged Access for Non-Security Functions                  | Configuring/modifying access authorizations (i.e., permissions, privileges);   | Functional     | Subset Of         | Non-Privileged Access for Non-Security Functions                  | IAC-21.2 | Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.  | 10                       |       |
| AC-6(2).d   | Non-Privileged Access for Non-Security Functions                  | Setting/modifying authentication parameters; and   | Functional     | Subset Of         | Non-Privileged Access for Non-Security Functions                  | IAC-21.2 | Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.  | 10                       |       |
| AC-6(2).e   | Non-Privileged Access for Non-Security Functions                  | Setting/modifying system configurations and parameters.  | Functional     | Subset Of         | Non-Privileged Access for Non-Security Functions                  | IAC-21.2 | Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.  | 10                       |       |
| AC-6(2)-1.1 | Non-Privileged Access for Non-Security Functions                  | For service providers, the organization requires that users of information system accounts, or roles, with access to all security functions, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audit any use of privileged accounts, or roles, for such functions.  | Functional     | Subset Of         | Non-Privileged Access for Non-Security Functions                  | IAC-21.2 | Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.  | 10                       |       |
| AC-6(5)     | Privileged Accounts   | The organization restricts privileged accounts on the information system to defined personnel or roles (defined in the applicable security plan).  | Functional     | Subset Of         | 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-6(9)     | Auditing Use of Privileged Functions                              | The information system audits the execution of privileged functions.   | Functional     | Subset Of         | Auditing Use of Privileged Functions                              | IAC-21.4 | Mechanisms exist to audit the execution of privileged functions.  | 10                       |       |
| AC-6(10)    | Prohibit Non-Privileged Users from Executing Privileged Functions | The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.<br>The information system:  | Functional     | Subset Of         | Prohibit Non-Privileged Users from Executing Privileged Functions | IAC-21.5 | Mechanisms exist to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards/countermeasures.   | 10                       |       |
| AC-7        | Unsuccessful Logon Attempts                                       | The information system:  | Functional     | Subset Of         | Account Lockout   | IAC-22   | Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded. | 10                       |       |
| AC-7.a      | Unsuccessful Logon Attempts                                       | Enforces the limit of consecutive invalid login attempts by a user specified in the implementation Standard during the time period specified in the implementation Standard; and   | Functional     | Subset Of         | Account Lockout   | IAC-22   | Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded. | 10                       |       |
| AC-7.b      | Unsuccessful Logon Attempts                                       | Automatically disables or locks the account/role until released by an administrator or after the time period specified in the implementation Standard when the maximum number of unsuccessful attempts is exceeded.  | Functional     | Subset Of         | Account Lockout   | IAC-22   | Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded. | 10                       |       |
| AC-7-1.1    | Unsuccessful Logon Attempts                                       | Configure the information system to lock out the user account automatically after three (3) invalid login attempts through either a local or network connection during a fifteen (15)-minute time period. Require the lockout to persist for a minimum of thirty (30) minutes.   | Functional     | Subset Of         | 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-8        | System Use Notification   | The information system:  | Functional     | Subset Of         | 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 Technology Assets, Applications and/or Services (TAAS).          | 10                       |       |
| AC-8.a      | System Use Notification   | Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The approved banner states:<br>Warning! This system contains U.S. Government information. By using this information system, you are consenting to system monitoring for law enforcement and other purposes. Unauthorized or improper use of, or access to, this computer system may subject you to state and federal criminal prosecution and penalties as well as civil penalties. At any time, the government may intercept, search, and seize any communication or data transmitted or stored on this information system. | Functional     | Subset Of         | 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 Technology Assets, Applications and/or Services (TAAS).          | 10                       |       |
| AC-8.b      | System Use Notification   | Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and  | Functional     | Subset Of         | 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 Technology Assets, Applications and/or Services (TAAS).          | 10                       |       |
| AC-8.c      | System Use Notification   | For publicly accessible systems:   | Functional     | Subset Of         | 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 Technology Assets, Applications and/or Services (TAAS).          | 10                       |       |
| AC-8.c.1    | System Use Notification   | Displays system use information when appropriate, before granting further access;  | Functional     | Subset Of         | 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 Technology Assets, Applications and/or Services (TAAS).          | 10                       |       |

| FDE #       | FDE Name   | Focal Document Element (FDE) Description   | STRM Rationale | STRM Relationship | SCF Control  | SCF #    | Secure Controls Framework (SCF) Control Description   | Strength of Relationship | Notes |
|-------------|--|--|----------------|-------------------|--|----------|---|--------------------------|-------|
| AC-8-c.2    | System Use Notification                                    | Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and  | Functional     | Subset Of         | 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 Technology Assets, Applications and/or Services (TAAS).   | 10                       |       |
| AC-8-c.3    | System Use Notification                                    | Includes a description of the authorized uses of the system.   | Functional     | Subset Of         | 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 Technology Assets, Applications and/or Services (TAAS).   | 10                       |       |
| AC-8-5.1    | System Use Notification                                    | The System Owner determines elements of the environment that require the System Use Notification control.  | Functional     | Subset Of         | Secure Baseline Configurations                             | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| AC-8-5.2    | System Use Notification                                    | The System Owner determines how System Use Notification will be verified and provides appropriate periodicity of the check.  | Functional     | Subset Of         | Secure Baseline Configurations                             | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| AC-8-5.3    | System Use Notification                                    | If not performed as part of a Configuration Baseline check, the organization has a documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider.   | Functional     | Subset Of         | Secure Baseline Configurations                             | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| AC-10       | Concurrent Session Control                                 | The information system limits the number of concurrent sessions for each system account to one (1) session. The number of concurrent application/process sessions is limited and enforced to the number of sessions expressly required for the performance of job duties and any requirement for more than one (1) concurrent application/process session is documented in the security plan.                | Functional     | Subset Of         | Concurrent Session Control                                 | IAC-23   | Mechanisms exist to limit the number of concurrent sessions for each system account.  | 10                       |       |
| AC-11       | Session Lock   | The information system:  | Functional     | Intersects With   | Session Lock   | IAC-24   | Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods. | 5                        |       |
| AC-11.a     | Session Lock   | Prevents further access to the system by initiating a session lock after fifteen (15) minutes of inactivity or upon receiving a request from a user; and   | Functional     | Subset Of         | Session Lock   | IAC-24   | Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods. | 10                       |       |
| AC-11.b     | Session Lock   | Retains the session lock until the user reestablishes access using established identification and authentication procedures.   | Functional     | Subset Of         | Session Lock   | IAC-24   | Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods. | 10                       |       |
| AC-11(1)    | Pattern-Hiding Displays                                    | The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.   | Functional     | Subset Of         | Pattern-Hiding Displays                                    | IAC-24.1 | Mechanisms exist to implement pattern-hiding displays to conceal information previously visible on the display during the session lock.   | 10                       |       |
| AC-12       | Session Termination  | The information system automatically terminates a user session after fifteen (15) minutes of inactivity.   | Functional     | Subset Of         | Session Termination  | IAC-25   | Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.  | 10                       |       |
| AC-14       | Permitted Actions Without Identification or Authentication | The organization:  | Functional     | Subset Of         | Permitted Actions Without Identification or Authentication | 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.a     | Permitted Actions Without Identification or Authentication | Identifies, documents, and provides supporting rationale in the system security plan for user actions not requiring identification or authentication; and  | Functional     | Subset Of         | Permitted Actions Without Identification or Authentication | 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.b     | Permitted Actions Without Identification or Authentication | Configures information systems to permit public access without first requiring individual identification and authentication only to the extent necessary to accomplish mission objectives.   | Functional     | Subset Of         | Permitted Actions Without Identification or Authentication | IAC-26   | Mechanisms exist to identify and document the supporting rationale for specific user actions that can be performed on a system without identification or authentication.  | 10                       |       |
| AC-17       | Remote Access  | N/A  | Functional     | Intersects With   | Remote Access  | NET-14   | Mechanisms exist to define, control and review organization-approved, secure remote access methods.   | 5                        |       |
| AC-17.a     | Remote Access  | The organization monitors for unauthorized remote access to the information. Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be explicitly authorized, in writing, by the organization's CIO or the designated representative. If authorized, the organization:  | Functional     | Subset Of         | Remote Access  | NET-14   | Mechanisms exist to define, control and review organization-approved, secure remote access methods.   | 10                       |       |
| AC-17.a.1   | Remote Access  | Documents allowed methods of remote access to the information system;  | Functional     | Subset Of         | Remote Access  | NET-14   | Mechanisms exist to define, control and review organization-approved, secure remote access methods.   | 10                       |       |
| AC-17.a.2   | Remote Access  | Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed;   | Functional     | Subset Of         | Remote Access  | NET-14   | Mechanisms exist to define, control and review organization-approved, secure remote access methods.   | 10                       |       |
| AC-17.a.3   | Remote Access  | Authorizes remote access to the information system prior to allowing such connections; and   | Functional     | Subset Of         | Remote Access  | NET-14   | Mechanisms exist to define, control and review organization-approved, secure remote access methods.   | 10                       |       |
| AC-17.b     | Remote Access  | Monitors for unauthorized remote access to the information system.   | Functional     | Subset Of         | Remote Access  | NET-14   | Mechanisms exist to define, control and review organization-approved, secure remote access methods.   | 10                       |       |
| AC-17-5.1   | Remote Access  | Require callback capability with re-authentication to verify connections from authorized locations when a secure data communications service network cannot be used.   | Functional     | Subset Of         | Remote Access  | NET-14   | Mechanisms exist to define, control and review organization-approved, secure remote access methods.   | 10                       |       |
| AC-17-5.2   | Remote Access  | All computers and devices, whether organization-furnished equipment or contractor-furnished equipment, that require any network access to a network or system are securely configured and meet at least the following security requirements: (i) up-to-date system patches, (ii) current anti-virus software, and (iii) functionality that provides the capability for automatic execution of code disabled. | Functional     | Subset Of         | Secure Baseline Configurations                             | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| AC-17-5.3   | Remote Access  | Remote connection for privileged functions must be performed using multi-factor authentication following Electronic Authentication Guidelines for ACA Administering Entity Systems, which can be found at: <a href="https://cait.cms.gov/sf/projects/cms_aca_program_security_privacy/">https://cait.cms.gov/sf/projects/cms_aca_program_security_privacy/</a>   | Functional     | Subset Of         | Remote Access  | NET-14   | Mechanisms exist to define, control and review organization-approved, secure remote access methods.   | 10                       |       |
| AC-17(1)    | Automated Monitoring/Control                               | The information system monitors and controls remote access methods.  | Functional     | Subset Of         | Automated Monitoring & Control                             | NET-14.1 | Automated mechanisms exist to monitor and control remote access sessions.   | 10                       |       |
| AC-17(2)    | Protection of Confidentiality/Integrity Using Encryption   | The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.   | Functional     | Subset Of         | 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(3)    | Managed Access Control Points                              | The information system routes all remote accesses through a limited number of managed access control points.   | Functional     | Subset Of         | 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(4)    | Privileged Commands/Access                                 | The organization:  | Functional     | Subset Of         | 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(4.a)  | Privileged Commands/Access                                 | Authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs; and   | Functional     | Subset Of         | 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(4.b)  | Privileged Commands/Access                                 | Documents the rationale for such access in the security plan for the information system.   | Functional     | Subset Of         | 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-18       | Wireless Access  | The organization:  | Functional     | Intersects With   | Wireless Networking  | NET-15   | Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.   | 5                        |       |
| AC-18       | Wireless Access  | The organization:  | Functional     | Intersects With   | Wireless Access Authentication & Encryption                | CRY-07   | Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.   | 5                        |       |
| AC-18.a     | Wireless Access  | Prohibits the installation of wireless access points (WAP) to information systems unless explicitly authorized, in writing, by the organization CIO or a designated representative.  | Functional     | Subset Of         | Wireless Networking  | NET-15   | Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.   | 10                       |       |
| AC-18.b     | Wireless Access  | Monitors for unauthorized wireless access to information systems by employing a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system, and   | Functional     | Subset Of         | Wireless Networking  | NET-15   | Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.   | 10                       |       |
| AC-18.c     | Wireless Access  | Establishes for authorized wireless access usage restrictions, configuration/connection requirements, and implementation guidance for wireless access prior to allowing such connections.  | Functional     | Subset Of         | Wireless Networking  | NET-15   | Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.   | 10                       |       |
| AC-18-5.1   | Wireless Access  | If wireless access is explicitly authorized, wireless device service set identifier broadcasting is disabled and the following wireless restrictions and access controls are implemented:  | Functional     | Subset Of         | Secure Baseline Configurations                             | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| AC-18-5.1.a | Wireless Access  | Encryption protection is enabled;  | Functional     | Subset Of         | Secure Baseline Configurations                             | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| AC-18-5.1.b | Wireless Access  | Access points are placed in secure areas;  | Functional     | Subset Of         | Secure Baseline Configurations                             | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| AC-18-5.1.c | Wireless Access  | Access points are shut down when not in use (i.e., nights, weekends);  | Functional     | Subset Of         | Secure Baseline Configurations                             | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| AC-18-5.1.d | Wireless Access  | A firewall is implemented between the wireless network and the wired infrastructure;   | Functional     | Subset Of         | Secure Baseline Configurations                             | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| AC-18-5.1.e | Wireless Access  | MAC address authentication is utilized;  | Functional     | Subset Of         | Secure Baseline Configurations                             | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| AC-18-5.1.f | Wireless Access  | Static IP addresses, not DHCP, is utilized;  | Functional     | Subset Of         | Secure Baseline Configurations                             | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| AC-18-5.1.g | Wireless Access  | Personal firewalls are utilized on all wireless clients;   | Functional     | Subset Of         | Secure Baseline Configurations                             | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| AC-18-5.1.h | Wireless Access  | File sharing is disabled on all wireless clients;  | Functional     | Subset Of         | Secure Baseline Configurations                             | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| AC-18-5.1.i | Wireless Access  | Intrusion detection agents are deployed on the wireless side of the firewall;  | Functional     | Subset Of         | Secure Baseline Configurations                             | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| AC-18-5.1.j | Wireless Access  | Wireless activity is monitored and recorded, and the records are reviewed on a regular basis;  | Functional     | Subset Of         | Secure Baseline Configurations                             | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| AC-18-5.1.k | Wireless Access  | Organizational policy related to wireless client access configuration and use is documented; and   | Functional     | Subset Of         | Secure Baseline Configurations                             | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| AC-18-5.1.l | Wireless Access  | Security Control SI-4 (14), Employ a wireless intrusion "detection/prevention" system (WIDS/WIPS).   | Functional     | Subset Of         | Secure Baseline Configurations                             | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| AC-18(1)    | Authentication and Encryption                              | If wireless access is explicitly authorized, the information system protects wireless access to the system using encryption and authentication of both users and devices.  | Functional     | Subset Of         | Authentication & Encryption                                | NET-15.1 | Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by:(1) Authenticating devices trying to connect; and(2) Encrypting transmitted data.   | 10                       |       |

| FDE #         | FDE Name  | Focal Document Element (FDE) Description   | STRM Rationale | STRM Relationship | SCF Control  | SCF #    | Secure Controls Framework (SCF) Control Description   | Strength of Relationship | Notes                     |
|---------------|---|--|----------------|-------------------|--|----------|---|--------------------------|---------------------------|
| AC-19         | Access Control For Mobile Devices                     | The organization:  | Functional     | Subset Of         | 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.a       | Access Control For Mobile Devices                     | Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices;   | Functional     | Subset Of         | 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.b       | Access Control For Mobile Devices                     | Authorizes, through the CIO, the connection of mobile devices to organizational information systems;   | Functional     | Subset Of         | 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.c       | Access Control For Mobile Devices                     | Employs an approved method of cryptography (see SC-13) to protect Personally Identifiable Information (PII) residing on portable and mobile information devices, and utilizes whole-disk encryption solution for laptops;  | Functional     | Subset Of         | 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.d       | Access Control For Mobile Devices                     | Monitors for unauthorized connections of mobile devices to information systems;  | Functional     | Subset Of         | 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.e       | Access Control For Mobile Devices                     | Enforces requirements for the connection of mobile devices to information systems;   | Functional     | Subset Of         | 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.f       | Access Control For Mobile Devices                     | Disables information system functionality that provides for automatic execution of code on mobile devices without user direction;  | Functional     | Subset Of         | 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.g       | Access Control For Mobile Devices                     | Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and  | Functional     | Subset Of         | 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.h       | Access Control For Mobile Devices                     | Protects the storage and transmission of information on portable and mobile information devices with activities such as scanning the devices for malicious code and virus protection software;   | Functional     | Subset Of         | 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-IS.1    | Access Control For Mobile Devices                     | The organization defines inspection and preventive measures.   | Functional     | Subset Of         | 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-IS.2    | Access Control For Mobile Devices                     | Purge/wipe information from mobile devices based on ten (10) consecutive, unsuccessful device login attempts (e.g., personal digital assistants, smartphones, and tablets). Laptop computers are excluded from this requirement.   | Functional     | Subset Of         | Secure Baseline Configurations   | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |                           |
| AC-19-IS.3    | Access Control For Mobile Devices                     | Only organization-owned mobile devices and software can be used to process, access, and store PII.   | Functional     | Subset Of         | 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(S)      | Full-Device / Container-Based Encryption              | The organization employs full-device encryption, or container encryption, to protect the confidentiality and integrity of information on approved mobile devices.  | Functional     | Subset Of         | 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(S)-IS   | Full-Device / Container-Based Encryption              | For mobile devices containing Personally Identifiable Information (PII), employ encryption to protect the confidentiality and integrity of information on mobile devices (e.g., smartphones and laptop computers).   | Functional     | Subset Of         | Secure Baseline Configurations   | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |                           |
| AC-20         | Use of External Information Systems                   | For organizational users (staff and contractors within the organization), the organization prohibits the use of external information systems, including but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistants (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports to store, access, transmit, or process sensitive information, such as Personally Identifiable Information (PII), unless explicitly authorized, in writing, by the CIO or designated representative. If authorized, the organization establishes strict terms and conditions for their use. For non-organizational users (such as business partners), the Administering entity organization establishes terms and conditions, consistent with CMS implementation guidance of HHS Regulation 45 CFR 115.260, and in compliance with legal data sharing agreements signed with CMS, for any trust relationships established with other organizations owning, operating, and/or maintaining external information systems. These terms and conditions allow authorized individuals to: | Functional     | Subset Of         | Use of External Technology Assets, Applications and/or Services (TAAS) | DCH-13   | Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.   | 10                       |                           |
| AC-20.a       | Use of External Information Systems                   | Access the information system from external information systems; and   | Functional     | Subset Of         | Use of External Technology Assets, Applications and/or Services (TAAS) | DCH-13   | Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.   | 10                       |                           |
| AC-20.b       | Use of External Information Systems                   | Process, store, or transmit organization-controlled information using external information system;   | Functional     | Subset Of         | Use of External Technology Assets, Applications and/or Services (TAAS) | DCH-13   | Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.   | 10                       |                           |
| AC-20-IS      | Use of External Information Systems                   | For Organizational Users:  | Functional     | Subset Of         | Use of External Technology Assets, Applications and/or Services (TAAS) | DCH-13   | Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.   | 10                       |                           |
| AC-20-IS.1    | Use of External Information Systems                   | Instruct all personnel working from a non-organization location to implement fundamental security controls and practices, including passwords, virus protection, and personal firewall is.   | Functional     | Subset Of         | Use of External Technology Assets, Applications and/or Services (TAAS) | DCH-13   | Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.   | 10                       |                           |
| AC-20-IS.2    | Use of External Information Systems                   | Limit remote access only to information resources required to complete job duties.   | Functional     | Subset Of         | Use of External Technology Assets, Applications and/or Services (TAAS) | DCH-13   | Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.   | 10                       |                           |
| AC-20-IS.3    | Use of External Information Systems                   | Only organization-owned computers and software can be used to process, access, and store Personally Identifiable Information (PII).  | Functional     | Subset Of         | Use of External Technology Assets, Applications and/or Services (TAAS) | DCH-13   | Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.   | 10                       |                           |
| AC-20(I)      | Limits on Authorized Use                              | The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:   | Functional     | Subset Of         | Limits of Authorized Use   | DCH-13.1 | Mechanisms exist to prohibit external parties, including Technology Assets, Applications and/or Services (TAAS), from storing, processing and transmitting data unless authorized individuals first: (1) Verifying the implementation of required security, compliance and/or resilience controls; or (2) Retaining a processing agreement with the entity hosting the external TAAS. | 10                       |                           |
| AC-20(I).a    | Limits on Authorized Use                              | Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or  | Functional     | Subset Of         | Limits of Authorized Use   | DCH-13.1 | Mechanisms exist to prohibit external parties, including Technology Assets, Applications and/or Services (TAAS), from storing, processing and transmitting data unless authorized individuals first: (1) Verifying the implementation of required security, compliance and/or resilience controls; or (2) Retaining a processing agreement with the entity hosting the external TAAS. | 10                       |                           |
| AC-20(I).b    | Limits on Authorized Use                              | Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.  | Functional     | Subset Of         | Limits of Authorized Use   | DCH-13.1 | Mechanisms exist to prohibit external parties, including Technology Assets, Applications and/or Services (TAAS), from storing, processing and transmitting data unless authorized individuals first: (1) Verifying the implementation of required security, compliance and/or resilience controls; or (2) Retaining a processing agreement with the entity hosting the external TAAS. | 10                       |                           |
| AC-20(2)      | Portable Storage Devices                              | The organization restricts the use of organization-controlled portable storage devices by authorized individuals on external information systems.  | 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(2)-IS.a | Portable Storage Devices                              | Only organization-owned portable storage devices can be used to process, access, and store Personally Identifiable Information. These devices should employ encryption to protect the confidentiality and integrity of information.  | Functional     | Intersects With   | Portable Storage Devices   | DCH-13.2 | Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.  | 5                        |                           |
| AC-21         | Information Sharing                                   | The organization:  | 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         | Information Sharing                                   | The organization:  | 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.a       | Information Sharing                                   | Facilitates information sharing as defined in 45 CFR 115.260 (e), Privacy and security of personally identifiable information, or "data sharing" by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for approved information-sharing circumstances (as defined in data sharing agreements such as the Computer Matching Agreement or Information Exchange Agreement) where user discretion is required; and  | Functional     | Subset Of         | Information Sharing  | DCH-14   | Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.  | 10                       |                           |
| AC-21.b       | Information Sharing                                   | Employs defined automated mechanisms or manual processes (defined in the applicable security plan) to assist users in making information sharing/collaboration decisions.  | Functional     | Subset Of         | Information Sharing  | DCH-14   | Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.  | 10                       |                           |
| AC-22         | Publicly Accessible Content                           | The organization:  | Functional     | Subset Of         | Publicly Accessible Content  | DCH-15   | Mechanisms exist to control publicly-accessible content.  | 10                       |                           |
| AC-22.a       | Publicly Accessible Content                           | Designates individuals authorized to post information onto a publicly accessible information system;   | Functional     | Subset Of         | Publicly Accessible Content  | DCH-15   | Mechanisms exist to control publicly-accessible content.  | 10                       |                           |
| AC-22.b       | Publicly Accessible Content                           | Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;   | Functional     | Subset Of         | Publicly Accessible Content  | DCH-15   | Mechanisms exist to control publicly-accessible content.  | 10                       |                           |
| AC-22.c       | Publicly Accessible Content                           | Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and   | Functional     | Subset Of         | Publicly Accessible Content  | DCH-15   | Mechanisms exist to control publicly-accessible content.  | 10                       |                           |
| AC-22.d       | Publicly Accessible Content                           | Reviews the content on the publicly accessible information system for nonpublic information bi-weekly and removes such information, if discovered.   | Functional     | Subset Of         | Publicly Accessible Content  | DCH-15   | Mechanisms exist to control publicly-accessible content.  | 10                       |                           |
| 1.2           | Awareness and Training (AT)                           | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control |
| AT-1          | Security Awareness and Training Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:  | Functional     | Intersects With   | Periodic Review & Update of Resilience Program                         | GOV-03   | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRIP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.  | 5                        |                           |
| AT-1          | Security Awareness and Training Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:  | Functional     | Subset Of         | Security, Compliance & Resilience-Minded Workforce                     | SAT-01   | Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.   | 10                       |                           |
| AT-1          | Security Awareness and Training Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:  | Functional     | Intersects With   | Publishing Security, Compliance & Resilience Documentation             | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.  | 5                        |                           |
| AT-1.a        | Security Awareness and Training Policy and Procedures | A security and privacy awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;  | Functional     | Subset Of         | Publishing Security, Compliance & Resilience Documentation             | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.  | 10                       |                           |
| AT-1.b        | Security Awareness and Training Policy and Procedures | Procedures to facilitate the implementation of the security and privacy awareness and training policy and associated security and privacy awareness and training controls;   | Functional     | Subset Of         | Standardized Operating Procedures (SOP)                                | OPS-01.1 | Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.   | 10                       |                           |
| AT-1.c        | Security Awareness and Training Policy and Procedures | Security and privacy awareness and training policy; and  | Functional     | Subset Of         | Publishing Security, Compliance & Resilience Documentation             | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.  | 10                       |                           |
| AT-1.d        | Security Awareness and Training Policy and Procedures | Security and privacy awareness and training procedures.  | Functional     | Subset Of         | Publishing Security, Compliance & Resilience Documentation             | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.  | 10                       |                           |
| AT-1.e        | Security Awareness and Training Policy and Procedures | Security and privacy awareness and training plan.  | Functional     | Subset Of         | Security, Compliance & Resilience-Minded Workforce                     | SAT-01   | Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.   | 10                       |                           |

| FDE #      | FDE Name  | Focal Document Element (FDE) Description  | STRM Rationale | STRM Relationship | SCF Control   | SCF #    | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes                     |
|------------|---|---|----------------|-------------------|---|----------|--|--------------------------|---------------------------|
| AT-1-5.1   | Security Awareness and Training Policy and Procedures | An Initial Security and Privacy awareness and training plan is developed and implemented that addresses all requirements of the security and privacy training program. This plan should cover required policies and procedures and a documented process for implementing basic privacy and awareness training for all organizational users and contractors that includes understanding potential indicators of insider threats. This plan should also include requirements for ensuring personnel with specific roles and responsibilities in information security and privacy undergo more detailed and audience specific security and privacy training. | Functional     | Subset Of         | Security, Compliance & Resilience-Minded Workforce                    | SAT-01   | Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.  | 10                       |                           |
| AT-2       | Security Awareness Training                           | The organization provides basic security and privacy awareness training to information system users (including managers, senior executives, and contractors).   | Functional     | Subset Of         | Security, Compliance & Resilience Awareness Training                  | SAT-02   | Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.  | 10                       |                           |
| AT-2.a     | Security Awareness Training                           | As part of initial training for new users prior to accessing any system's information.  | Functional     | Subset Of         | Security, Compliance & Resilience Awareness Training                  | SAT-02   | Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.  | 10                       |                           |
| AT-2.b     | Security Awareness Training                           | When required by system changes, and within every three hundred sixty-five (365) days thereafter.   | Functional     | Subset Of         | Security, Compliance & Resilience Awareness Training                  | SAT-02   | Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.  | 10                       |                           |
| AT-2-5.1   | Security Awareness Training                           | An information security and privacy education and awareness training program is developed and implemented for all employees and individuals working on behalf of the organization and involved in managing, using, and/or operating information systems.  | Functional     | Subset Of         | Security, Compliance & Resilience Awareness Training                  | SAT-02   | Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.  | 10                       |                           |
| AT-2-5.2   | Security Awareness Training                           | Security and privacy awareness training is provided before granting access to systems and networks, and within every three hundred sixty-five (365) days thereafter, to all employees and contractors to explain the importance and responsibility in safeguarding Personally Identifiable Information (PII) and ensuring privacy, as established in federal legislation and HHS Regulations and CMS and organization guidance.   | Functional     | Subset Of         | Security, Compliance & Resilience Awareness Training                  | SAT-02   | Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.  | 10                       |                           |
| AT-2(2)    | Insider Threat  | The organization includes security and privacy awareness training on recognizing and reporting potential indicators of insider threat.  | Functional     | Subset Of         | Insider Threat Awareness  | THR-05   | Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.   | 10                       |                           |
| AT-3       | Role-Based Security Training                          | The organization provides role-based security and privacy training to personnel with assigned security and privacy roles and responsibilities.  | Functional     | Intersects With   | Role-Based Security, Compliance & Resilience Training                 | SAT-03   | Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.   | 5                        |                           |
| AT-3.a     | Role-Based Security Training                          | Before authorizing access to the information system or performing assigned duties; and  | Functional     | Subset Of         | Role-Based Security, Compliance & Resilience Training                 | SAT-03   | Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.   | 10                       |                           |
| AT-3.b     | Role-Based Security Training                          | When required by information system changes, and with in every three hundred sixty-five (365) days thereafter.  | Functional     | Subset Of         | Role-Based Security, Compliance & Resilience Training                 | SAT-03   | Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.   | 10                       |                           |
| AT-3-5.1   | Role-Based Security Training                          | Require personnel with significant information security and privacy roles and responsibilities to undergo appropriate information system security and privacy training prior to authorizing access to networks, systems, and/or applications; when required by significant information system or system environment changes; when an employee enters a new position that requires additional role-specific training; and for refresher training with in every three hundred sixty-five (365) days thereafter.   | Functional     | Subset Of         | Role-Based Security, Compliance & Resilience Training                 | SAT-03   | Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties;(2) When required by system changes; and(3) Annually thereafter.   | 10                       |                           |
| AT-4       | Security Training Records                             | The organization:   | Functional     | Subset Of         | Security, Compliance & Resilience Training Records                    | SAT-04   | Mechanisms exist to document, retain and monitor individual training activities, including:(1) Initial security, compliance and resilience awareness training;(2) Recurring awareness training; and(3) Technology Assets, Applications and/or Services (TAAS)-specific training. | 10                       |                           |
| AT-4.a     | Security Training Records                             | Documents and monitors individual information system security and privacy training activities including basic security and privacy awareness training and specific information system security and privacy training; and  | Functional     | Subset Of         | Security, Compliance & Resilience Training Records                    | SAT-04   | Mechanisms exist to document, retain and monitor individual training activities, including:(1) Initial security, compliance and resilience awareness training;(2) Recurring awareness training; and(3) Technology Assets, Applications and/or Services (TAAS)-specific training. | 10                       |                           |
| AT-4.b     | Security Training Records                             | Retains individual training records for a minimum of five (5) years.  | Functional     | Subset Of         | Security, Compliance & Resilience Training Records                    | SAT-04   | Mechanisms exist to document, retain and monitor individual training activities, including:(1) Initial security, compliance and resilience awareness training;(2) Recurring awareness training; and(3) Technology Assets, Applications and/or Services (TAAS)-specific training. | 10                       |                           |
| 1.3        | Audit and Accountability (AU)                         | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control |
| AU-1       | Audit and Accountability Policy and Procedures        | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:   | Functional     | Intersects With   | Periodic Review & Update of Security, Compliance & Resilience Program | GOV-03   | Mechanisms exist to review the Security, Compliance & Resilience Program (including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.                                 | 5                        |                           |
| AU-1       | Audit and Accountability Policy and Procedures        | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:   | Functional     | Intersects With   | Publishing Security, Compliance & Resilience Documentation            | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.   | 5                        |                           |
| AU-1       | Audit and Accountability Policy and Procedures        | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:   | Functional     | Subset Of         | Continuous Monitoring   | MON-01   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.  | 10                       |                           |
| AU-1.a     | Audit and Accountability Policy and Procedures        | An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and   | Functional     | Subset Of         | Publishing Security, Compliance & Resilience Documentation            | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.   | 10                       |                           |
| AU-1.b     | Audit and Accountability Policy and Procedures        | Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.  | Functional     | Subset Of         | Standardized Operating Procedures (SOP)                               | OPS-01.1 | Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.  | 10                       |                           |
| AU-2       | Audit Events  | The organization:   | Functional     | Intersects With   | Security Event Monitoring   | MON-01.8 | Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.  | 5                        |                           |
| AU-2       | Audit Events  | The organization:   | Functional     | Intersects With   | Centralized Collection of Security Event Logs                         | MON-02   | Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.   | 5                        |                           |
| AU-2.a     | Audit Events  | Determines, based on a risk assessment and mission/business needs, that the information system is capable of auditing the events specified in the Implementation Standards;   | Functional     | Subset Of         | 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.   | 10                       |                           |
| AU-2.b     | Audit Events  | Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; and   | Functional     | Subset Of         | 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.   | 10                       |                           |
| AU-2.c     | Audit Events  | Determines, based on current threat information and ongoing assessment of risk, which events require auditing on a continuous basis and which events require auditing in response to specific situations.   | Functional     | Subset Of         | 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.   | 10                       |                           |
| AU-2-5.1   | Audit Events  | Generate audit records for the following auditable events:  | Functional     | Subset Of         | Secure Baseline Configurations  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |                           |
| AU-2-5.1.a | Audit Events  | Server alerts and error messages;   | Functional     | Subset Of         | Secure Baseline Configurations  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |                           |
| AU-2-5.1.b | Audit Events  | Log onto system;  | Functional     | Subset Of         | Secure Baseline Configurations  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |                           |
| AU-2-5.1.c | Audit Events  | Log off system;   | Functional     | Subset Of         | Secure Baseline Configurations  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |                           |
| AU-2-5.1.d | Audit Events  | Change of password;   | Functional     | Subset Of         | Secure Baseline Configurations  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |                           |
| AU-2-5.1.e | Audit Events  | All system administrator commands, while logged on as system administrator;   | Functional     | Subset Of         | Secure Baseline Configurations  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |                           |
| AU-2-5.1.f | Audit Events  | Switching accounts or running privileged actions from another account, (e.g., Linux/UNIX su or Windows RUNAS);  | Functional     | Subset Of         | Secure Baseline Configurations  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |                           |
| AU-2-5.1.g | Audit Events  | Creation or modification of super-user groups;  | Functional     | Subset Of         | Secure Baseline Configurations  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |                           |
| AU-2-5.1.h | Audit Events  | Subset of security administrator commands, while logged on in the security administrator role;  | Functional     | Subset Of         | Secure Baseline Configurations  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |                           |
| AU-2-5.1.i | Audit Events  | Subset of system administrator commands, while logged on in the user role;  | Functional     | Subset Of         | Secure Baseline Configurations  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |                           |
| AU-2-5.1.j | Audit Events  | Clearing of the audit log file;   | Functional     | Subset Of         | Secure Baseline Configurations  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |                           |
| AU-2-5.1.k | Audit Events  | Startup and shutdown of audit functions;  | Functional     | Subset Of         | Secure Baseline Configurations  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |                           |
| AU-2-5.1.l | Audit Events  | Use of identification and authentication mechanisms (e.g., user ID and password);   | Functional     | Subset Of         | Secure Baseline Configurations  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |                           |
| AU-2-5.1.m | Audit Events  | Change of file or user permissions or privileges (e.g., use of su/guid, chown, su);   | Functional     | Subset Of         | Secure Baseline Configurations  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |                           |
| AU-2-5.1.n | Audit Events  | Remote access outside of the corporate network communication channels(e.g., modems, dedicated Virtual Private Network ) and all dial-in access to the system;   | Functional     | Subset Of         | Secure Baseline Configurations  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |                           |
| AU-2-5.1.o | Audit Events  | Changes made to an applications or database by a batch file;  | Functional     | Subset Of         | Secure Baseline Configurations  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |                           |

| FDE #          | FDE Name                     | Focal Document Element (FDE) Description   | STRM Rationale | STRM Relationship | SCF Control                                 | SCF #    | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes |
|----------------|------------------------------|--|----------------|-------------------|---|----------|--|--------------------------|-------|
| AU-2-IS.1.p    | Audit Events                 | Application-critical record changes;   | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |       |
| AU-2-IS.1.q    | Audit Events                 | Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility);  | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |       |
| AU-2-IS.1.r    | Audit Events                 | User log-on and log-off (successful or unsuccessful);  | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |       |
| AU-2-IS.1.s    | Audit Events                 | System shutdown and reboot;  | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |       |
| AU-2-IS.1.t    | Audit Events                 | System errors;   | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |       |
| AU-2-IS.1.u    | Audit Events                 | Application shutdown;  | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |       |
| AU-2-IS.1.v    | Audit Events                 | Application restart;   | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |       |
| AU-2-IS.1.w    | Audit Events                 | Application errors;  | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |       |
| AU-2-IS.1.x    | Audit Events                 | Security policy modifications; and   | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |       |
| AU-2-IS.1.y    | Audit Events                 | Printing sensitive information.  | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |       |
| AU-2-IS.2      | Audit Events                 | Subset of Implementation Standard 1, Enable logging for perimeter devices, including firewalls and routers;  | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |       |
| AU-2-IS.2.a    | Audit Events                 | User log-on and log-off (successful or unsuccessful);  | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |       |
| AU-2-IS.2.b    | Audit Events                 | Log packet-screening denials originating from untrusted networks;  | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |       |
| AU-2-IS.2.c    | Audit Events                 | All system administration activities;  | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |       |
| AU-2-IS.2.d    | Audit Events                 | Packet-screening denials originating from trusted networks;  | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |       |
| AU-2-IS.2.e    | Audit Events                 | Account creation, modification, or deletion of packet filters;   | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |       |
| AU-2-IS.2.f    | Audit Events                 | System shutdown and reboot;  | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |       |
| AU-2-IS.2.g    | Audit Events                 | System errors; and   | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |       |
| AU-2-IS.2.h    | Audit Events                 | Modification of proxy services.  | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |       |
| AU-2-IS.3      | Audit Events                 | Verify that proper logging is enabled to audit administrator activities.   | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |       |
| AU-2-IS.4      | Audit Events                 | U.S.C 552a(c) Accounting of Certain Disclosures: Each agency shall keep an accurate accounting of the date, nature and purpose of each disclosure of a record to any person/entity or other agency and the name and address of the person/entity or agency to whom the disclosure is made. The agency must retain the accounting for at least five years or the life of the record whichever is longer after the disclosure for which the accounting is made; make the accounting available to the individual named in the record at his request; and inform any person/entity or other agency about any correction or notation of dispute made by the agency of any record that has been disclosed to the person or agency if an accounting of the disclosure was made. | Functional     | Intersects With   | Accounting of Disclosures                   | PR1-14.1 | Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by (1) The organization, and/or (2) Relevant third-parties that their PD was shared with.   | 5                        |       |
| AU-2(3)        | Reviews and Updates          | The organization reviews and updates the list of auditable events within every three hundred sixty-five (365) days or whenever there is change in the threat environment.  | Functional     | Subset Of         | Centralized Management of Event Log Content | MON-03.6 | Mechanisms exist to centrally manage and update the criteria to be captured in event logs generated by organization-defined system components.   | 10                       |       |
| AU-2(3)-IS.1   | Reviews and Updates          | The System Owner reviews and approves the list of auditable events.  | Functional     | Subset Of         | Centralized Management of Event Log Content | MON-03.6 | Mechanisms exist to centrally manage and update the criteria to be captured in event logs generated by organization-defined system components.   | 10                       |       |
| AU-3           | Content of Audit Records     | The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.   | Functional     | Subset Of         | 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-3(1)        | Additional Audit Information | The information system provides the capability to include more detailed information in the audit records for audit events that capture:  | Functional     | Subset Of         | Sensitive Event Log Information             | MON-03.1 | Mechanisms exist to protect sensitive/regulated data contained in log files.   | 10                       |       |
| AU-3(1).a      | Additional Audit Information | Filename accessed;   | Functional     | Subset Of         | 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-3(1).b      | Additional Audit Information | Program or command used to initiate the event; and   | Functional     | Subset Of         | 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-3(1).c      | Additional Audit Information | Source and destination addresses.  | Functional     | Subset Of         | 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-3(1)-IS.1   | Additional Audit Information | The information system includes:   | Functional     | Subset Of         | 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-3(1)-IS.1.a | Additional Audit Information | Additional, more detailed session, connection, transaction, or activity duration information;  | Functional     | Subset Of         | 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-3(1)-IS.1.b | Additional Audit Information | For client-server transactions, the number of bytes received and bytes sent;   | Functional     | Subset Of         | 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                       |       |

| FDE #         | FDE Name  | Focal Document Element (FDE) Description  | STRM Rationale | STRM Relationship | SCF Control                                    | SCF #    | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes                     |
|---------------|---|---|----------------|-------------------|--|----------|--|--------------------------|---------------------------|
| AU-311-HS.1.c | Additional Audit Information                                  | Additional informational messages to diagnose or identify the event; and  | Functional     | Subset Of         | 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-311-HS.1.d | Additional Audit Information                                  | Characteristics that describe or identify the object or resource acted upon in the audit records for audit events identified by type, location, or subject.   | Functional     | Subset Of         | 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-311-HS.2   | Additional Audit Information                                  | The organization defines audit record types. The audit record types are approved and accepted by the System Owner.  | Functional     | Subset Of         | 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-4          | Audit Storage Capacity  | The organization allocates audit record storage capacity and configures auditing to reduce the likelihood that storage capacity will be exceeded.   | Functional     | Subset Of         | 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-5          | Response to Audit Processing Failures                         | The information system alerts designated personnel or roles (defined in the applicable security plan) in the event of an audit processing failure.  | Functional     | Subset Of         | 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-5(1)       | Audit Storage Capacity  | The information system provides a warning and alerts key personnel, roles, and/or locations (defined in the applicable security plan), within a defined time period (defined in the applicable security plan), when allocated audit record storage volume reaches 80 percent of the repository's maximum audit record storage capacity. | Functional     | Subset Of         | 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-6          | Audit Review, Analysis, and Reporting                         | The organization:   | Functional     | Intersects With   | Centralized Collection of Security Event Logs  | MON-02   | Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.   | 5                        |                           |
| AU-6          | Audit Review, Analysis, and Reporting                         | The organization:   | Functional     | Intersects With   | Audit Level Adjustments                        | MON-02.6 | Mechanisms exist to adjust the level of audit review, analysis and reporting based on evolving threat information from law enforcement, industry associations or other credible sources of threat intelligence.  | 5                        |                           |
| AU-6.a        | Audit Review, Analysis, and Reporting                         | Reviews and analyzes information system audit records regularly for indications of inappropriate or unusual activity; and reports findings to designated organizational officials (defined in the applicable security plan); and  | Functional     | Intersects With   | Centralized Collection of Security Event Logs  | MON-02   | Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.   | 5                        |                           |
| AU-6.b        | Audit Review, Analysis, and Reporting                         | Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in threat environment including operations, assets, individuals, other organizations, or the Nation 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-6-IS.1     | Audit Review, Analysis, and Reporting                         | Review system records for initialization sequences, logons, and errors; system processes and performance; and system resources utilization to determine anomalies on demand but no less than once with in a twenty-four (24) hour period. Generate alert notification for technical personnel review and assessment.                    | Functional     | Subset Of         | Security Event Monitoring                      | MON-01.8 | Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.  | 10                       |                           |
| AU-6-IS.2     | Audit Review, Analysis, and Reporting                         | Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical personnel review and assessment.   | Functional     | Subset Of         | Security Event Monitoring                      | MON-01.8 | Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.  | 10                       |                           |
| AU-6-IS.3     | Audit Review, Analysis, and Reporting                         | Investigate suspicious activity or suspected violations on the information system, and report findings to appropriate officials and take appropriate action.  | Functional     | Subset Of         | Security Event Monitoring                      | MON-01.8 | Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.  | 10                       |                           |
| AU-6-IS.4     | Audit Review, Analysis, and Reporting                         | Use automated utilities to review audit records at least once weekly for unusual, unexpected, or suspicious behavior.   | Functional     | Subset Of         | Security Event Monitoring                      | MON-01.8 | Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.  | 10                       |                           |
| AU-6-IS.5     | Audit Review, Analysis, and Reporting                         | Inspect administrator groups on demand but at least once every fourteen (14) days to ensure unauthorized administrator accounts have not been created.  | Functional     | Subset Of         | Security Event Monitoring                      | MON-01.8 | Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.  | 10                       |                           |
| AU-6-IS.6     | Audit Review, Analysis, and Reporting                         | Perform manual reviews of system audit records randomly on demand but at least once every thirty (30) days.   | Functional     | Subset Of         | Security Event Monitoring                      | MON-01.8 | Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.  | 10                       |                           |
| AU-6-IS.7     | Audit Review, Analysis, and Reporting                         | For service providers, the organization reviews and analyzes information system audit records at least weekly for indications of inappropriate or unusual activity, and reports findings to designated organizational officials.  | Functional     | Subset Of         | Security Event Monitoring                      | MON-01.8 | Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.  | 10                       |                           |
| AU-6(1)       | Process Integration   | The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.   | Functional     | Intersects With   | Sensitive Event Log Information                | MON-03.1 | Mechanisms exist to protect sensitive/regulated data contained in log files.   | 5                        |                           |
| AU-6(3)       | Correlate Audit Repositories                                  | The organization analyzes and correlates 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-7          | Audit Reduction and Report Generation                         | The information system provides an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and   | 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-7.a        | Audit Reduction and Report Generation                         | Does not alter the original content or time marking of audit records.   | Functional     | Subset Of         | Monitoring Reporting                           | MON-06   | Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.  | 10                       |                           |
| AU-7.b        | Audit Reduction and Report Generation                         | The information system provides the capability to process audit records for events of interest based on selectable event criteria.  | 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-7(1)       | Automatic Processing  | N/A   | Functional     | Intersects With   | Clock Synchronization                          | SEA-20   | Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.   | 5                        |                           |
| AU-8          | Time Stamps   | N/A   | 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-8.a        | Time Stamps   | The information system: Uses internal system clocks to generate time stamps for audit records; and  | Functional     | Intersects With   | Clock Synchronization                          | SEA-20   | Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.   | 5                        |                           |
| AU-8.b        | Time Stamps   | Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).  | 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-8(1)       | Synchronization with Authoritative Time Source                | The information system synchronizes the internal clocks to the authoritative time source when the time difference is greater than thirty (30) seconds.  | Functional     | Intersects With   | Clock Synchronization                          | SEA-20   | Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.   | 5                        |                           |
| AU-8(1)-HS.1  | Synchronization with Authoritative Time Source                | The information system synchronizes internal information system clocks at least hourly with: http://tf.nist.gov/tf-cg/servers.cgi   | Functional     | Intersects With   | Clock Synchronization                          | SEA-20   | Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.   | 5                        |                           |
| AU-8(1)-HS.2  | Synchronization with Authoritative Time Source                | The organization selects primary and secondary time servers used by the National Institute of Standards and Technology (NIST) Internet time service. The secondary server is selected from a different geographic region than the primary server.   | Functional     | Subset Of         | Secure Baseline Configurations                 | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |                           |
| AU-8(1)-HS.3  | Synchronization with Authoritative Time Source                | The organization synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server.   | Functional     | Subset Of         | Secure Baseline Configurations                 | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |                           |
| AU-9          | Protection of Audit Information                               | The information system protects audit information and audit tools from unauthorized access, modification, and deletion.   | Functional     | Subset Of         | Protection of Event Logs                       | MON-08   | Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.  | 10                       |                           |
| AU-9(4)       | Access by Subset of Privileged Users                          | The organization authorizes access to management of audit functionality to only those individuals or roles who are not subject to audit by that system, and defines this access in the applicable security plan.  | Functional     | Subset Of         | Access by Subset of Privileged Users           | MON-08.2 | Mechanisms exist to restrict access to the management of event logs to privileged users with a specific business need.   | 10                       |                           |
| AU-10         | Non-Repudiation   | The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed a particular action.  | Functional     | Subset Of         | Non-Repudiation                                | MON-09   | Mechanisms exist to utilize a non-repudiation capability to protect against an individual falsely denying having performed a particular action.  | 10                       |                           |
| AU-11         | Audit Record Retention  | The organization retains audit records online for at least ninety (90) days and archives old records for ten (10) years to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.  | Functional     | Subset Of         | 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-HS.1    | Audit Record Retention  | Audit inspection reports, including a record of corrective actions, are retained by the organization for a minimum of three (3) years from the date the inspection was completed.   | Functional     | Subset Of         | 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-HS.2    | Audit Record Retention  | The organization retains audit records online for at least ninety (90) days and further preserves audit records off-line for a period of ten (10) years.  | Functional     | Subset Of         | 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-12         | Audit Generation  | The information system:   | 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.a       | Audit Generation  | Provides audit record generation capability for all auditable events defined in AU-2 and associated implementation standards including requirements of 5 U.S.C. 552a(c), Accounting of Certain Disclosures.   | Functional     | Subset Of         | Monitoring Reporting                           | MON-06   | Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.  | 10                       |                           |
| AU-12.b       | Audit Generation  | Allows defined personnel or roles (defined in the applicable security plan) to select which auditable events are to be audited by specific components of the information system; and  | Functional     | Subset Of         | Monitoring Reporting                           | MON-06   | Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.  | 10                       |                           |
| AU-12.c       | Audit Generation  | Generates audit records for the list of events defined in AU-2 with the content defined in AU-3.  | Functional     | Subset Of         | Monitoring Reporting                           | MON-06   | Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.  | 10                       |                           |
| AU-12(5)      | Audit Generation  | The information system provides audit record generation capability for the list of auditable events defined in AU-2 at all information system components where audit information is deployed.   | Functional     | Subset Of         | Monitoring Reporting                           | MON-06   | Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.  | 10                       |                           |
| AU-12(1)      | System-Wide/Time-Correlated Audit Trail                       | The information system compiles audit records from defined information system components (defined in the applicable security plan) into a system-wide (logical or physical), time-correlated audit trail.   | Functional     | Subset Of         | 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-16         | Cross-Organizational Auditing                                 | The organization employs organization-defined methods for coordinating organization-defined audit information among external organizations when audit information is transmitted across organizational boundaries.  | Functional     | Intersects With   | Cross-Organizational Monitoring                | MON-14   | Mechanisms exist to coordinate sanitized event logs among external organizations to identify anomalous events when event logs are shared across organizational boundaries, without giving away sensitive or critical business data.  | 5                        |                           |
| 1.4           | Security Assessment and Authorization (CA)                    | N/A   | Functional     | No Relationship   | N/A  | N/A      | N/A  | 0                        | No applicable SCF control |
| CA-1          | Security Assessment and Authorization Policies and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within three hundred sixty-five (365) days:   | Functional     | Subset Of         | Information Assurance (IA) Operations          | IAO-01   | Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.  | 10                       |                           |
| CA-1          | Security Assessment and Authorization Policies and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within three hundred sixty-five (365) days:   | Functional     | Intersects With   | Periodic Review & Update of Resilience Program | GOV-03   | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.  | 5                        |                           |

| FDE #      | FDE Name  | Focal Document Element (FDE) Description   | STRM Rationale | STRM Relationship | SCF Control   | SCF #    | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes |
|------------|---|--|----------------|-------------------|---|----------|--|--------------------------|-------|
| CA-1       | Security Assessment and Authorization Policies and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within three hundred sixty-five (365) days;  | Functional     | Intersects With   | Publishing Security, Compliance & Resilience Documentation      | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.   | 5                        |       |
| CA-1.a     | Security Assessment and Authorization Policies and Procedures | A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;  | Functional     | Subset Of         | Publishing Security, Compliance & Resilience Documentation      | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.   | 10                       |       |
| CA-1.b     | Security Assessment and Authorization Policies and Procedures | Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls;   | Functional     | Subset Of         | Standardized Operating Procedures (SOP)                         | OPS-01.1 | Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.  | 10                       |       |
| CA-1.c     | Security Assessment and Authorization Policies and Procedures | Security assessment and authorization policy; and  | Functional     | Subset Of         | Publishing Security, Compliance & Resilience Documentation      | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.   | 10                       |       |
| CA-1.d     | Security Assessment and Authorization Policies and Procedures | Security assessment and authorization procedures.  | Functional     | Subset Of         | Standardized Operating Procedures (SOP)                         | OPS-01.1 | Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.  | 10                       |       |
| CA-2       | Security Assessments  | The organization:  | Functional     | Intersects With   | Functional Review Of Security, Compliance & Resilience Controls | CPL-03.2 | Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.   | 5                        |       |
| CA-2       | Security Assessments  | The organization:  | Functional     | Intersects With   | Technical Verification  | IAO-06   | Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and/or resilience controls.  | 5                        |       |
| CA-2       | Security Assessments  | The organization:  | Functional     | Intersects With   | Security, Compliance & Resilience in Project Management         | PRM-04   | Mechanisms exist to assess security, compliance and resilience controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.   | 5                        |       |
| CA-2       | Security Assessments  | The organization:  | Functional     | Intersects With   | Assessments   | IAO-02   | Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.  | 5                        |       |
| CA-2       | Security Assessments  | The organization:  | Functional     | Intersects With   | Security, Compliance & Resilience Assessments                   | CPL-03   | Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.  | 5                        |       |
| CA-2.a     | Security Assessments  | Develops a security and privacy assessment plan that describes the scope of the assessment including:  | Functional     | Subset Of         | Assessments   | IAO-02   | Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.  | 10                       |       |
| CA-2.a.1   | Security Assessments  | Security and privacy controls and control enhancements under assessment;   | Functional     | Subset Of         | Assessments   | IAO-02   | Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.  | 10                       |       |
| CA-2.a.2   | Security Assessments  | Assessment procedures to be used to determine control effectiveness; and   | Functional     | Subset Of         | Assessments   | IAO-02   | Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.  | 10                       |       |
| CA-2.a.3   | Security Assessments  | Assessment environment, assessment team, and assessment roles and responsibilities;  | Functional     | Subset Of         | Assessments   | IAO-02   | Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.  | 10                       |       |
| CA-2.b     | Security Assessments  | Assesses the security and privacy controls in the information system and its environment of operation within every three hundred sixty-five (365) days in accordance with the current Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges, 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 requirements;   | Functional     | Subset Of         | Assessments   | IAO-02   | Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.  | 10                       |       |
| CA-2.c     | Security Assessments  | Produces an assessment report that documents the results of the assessment; and  | Functional     | Subset Of         | Assessments   | IAO-02   | Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.  | 10                       |       |
| CA-2.d     | Security Assessments  | Provides the results of the security and privacy control assessment within every three hundred sixty-five (365) days, in writing, to the Business Owner who is responsible for reviewing the assessment documentation and updating system security documentation where necessary to reflect any changes to the system.   | Functional     | Subset Of         | Assessments   | IAO-02   | Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.  | 10                       |       |
| CA-2.1     | Security Assessments  | An independent assessment of all security and privacy controls must be conducted before the Administering Entity's (AE) Authorizing Official issues the authority to operate for all newly implemented, or significantly changed, systems.   | Functional     | Subset Of         | Assessments   | IAO-02   | Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.  | 10                       |       |
| CA-2.1.2   | Security Assessments  | CMS requires that an independent assessment of all security and privacy controls be conducted every three (3) years or with each major system change   | Functional     | Subset Of         | Assessments   | IAO-02   | Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.  | 10                       |       |
| CA-2.1.3   | Security Assessments  | The annual security and privacy assessment requirement mandated by CMS requires all security and privacy controls attributable to a system to be assessed over a three (3)-year period. To meet this requirement, a subset of the security and privacy controls shall be tested each year so that all controls are tested during a three (3)-year period. CMS provides guidance for conducting annual security and privacy assessments in the document, Annual Security and Privacy Assessment Procedures for Statebased ACA Administering Entity Systems found at <a href="https://calt.cms.gov/projects/cms_aca_program_security_privacy/">https://calt.cms.gov/projects/cms_aca_program_security_privacy/</a> . | Functional     | Subset Of         | Assessments   | IAO-02   | Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.  | 10                       |       |
| CA-2.1.4   | Security Assessments  | The Business Owner notifies CMS within thirty (30) days whenever updates are made to system security and privacy authorization artifacts or when significant role changes occur.   | Functional     | Subset Of         | Assessments   | IAO-02   | Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.  | 10                       |       |
| CA-2(1)    | Independent Assessors   | The organization employs assessors or assessment teams with CMS-defined level of independence to conduct security and privacy control assessments of the organization's information system.  | Functional     | Subset Of         | Assessor Independence   | IAO-02.1 | Mechanisms exist to ensure assessors or assessment teams have the appropriate independence to conduct security, compliance and/or resilience control assessments.  | 10                       |       |
| CA-2(1)-15 | Independent Assessors   | CMS provides guidance for employing independent assessors in the Framework of Independent Assessment (IA) of Security and Privacy Controls, located at: <a href="https://calt.cms.gov/projects/cms_aca_program_security_privacy/">https://calt.cms.gov/projects/cms_aca_program_security_privacy/</a> .  | Functional     | Subset Of         | Assessor Independence   | IAO-02.1 | Mechanisms exist to ensure assessors or assessment teams have the appropriate independence to conduct security, compliance and/or resilience control assessments.  | 10                       |       |
| CA-3       | System Interconnections                                       | The organization:  | Functional     | Intersects With   | Interconnection Security Agreements (ISAs)                      | NET-05   | Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and; (3) The nature of the information communicated.   | 5                        |       |
| CA-3.a     | System Interconnections                                       | Authorizes connections from the organization's information system to other information systems through the use of interconnection security agreements (ISAs)   | Functional     | Subset Of         | Interconnection Security Agreements (ISAs)                      | NET-05   | Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and; (3) The nature of the information communicated.   | 10                       |       |
| CA-3.b     | System Interconnections                                       | Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and   | Functional     | Subset Of         | Interconnection Security Agreements (ISAs)                      | NET-05   | Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and; (3) The nature of the information communicated.   | 10                       |       |
| CA-3.c     | System Interconnections                                       | Reviews and updates the ISAs on an ongoing basis to verify enforcement of security requirements; and   | Functional     | Subset Of         | Interconnection Security Agreements (ISAs)                      | NET-05   | Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and; (3) The nature of the information communicated.   | 10                       |       |
| CA-3.d     | System Interconnections                                       | Establishes system-to-system connections with CMS through the Fed2NonFed ISA process.  | Functional     | Subset Of         | Interconnection Security Agreements (ISAs)                      | NET-05   | Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and; (3) The nature of the information communicated.   | 10                       |       |
| CA-3.1     | System Interconnections                                       | Record each system interconnection in the security plan for the system that is connected to the remote location.   | Functional     | Subset Of         | Interconnection Security Agreements (ISAs)                      | NET-05   | Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and; (3) The nature of the information communicated.   | 10                       |       |
| CA-3.1.2   | System Interconnections                                       | The ISA is updated following significant changes to the system, organization, or the nature of the electronic sharing of information that could impact the validity of the agreement.  | Functional     | Subset Of         | Interconnection Security Agreements (ISAs)                      | NET-05   | Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and; (3) The nature of the information communicated.   | 10                       |       |
| CA-3.1.3   | System Interconnections                                       | The Fed2NonFed ISA process is defined in the Fed2NonFed ISA template found at: <a href="https://calt.cms.gov/projects/cms_aca_program_security_privacy/">https://calt.cms.gov/projects/cms_aca_program_security_privacy/</a> .   | Functional     | Subset Of         | Interconnection Security Agreements (ISAs)                      | NET-05   | Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and; (3) The nature of the information communicated.   | 10                       |       |
| CA-3(15)   | Restrictions on External System Connections                   | The organization employs, and documents, in the applicable security plan a "deny all, allow-by-exception" policy for allowing defined information systems that receive, process, store, or transmit Personally Identifiable Information (PII) to connect to external information systems.  | Functional     | Intersects With   | External System Connections                                     | NET-05.1 | Mechanisms exist to prohibit the direct connection of a sensitive system to an external network without the use of an organization-defined boundary protection device.   | 5                        |       |
| CA-5       | Plan of Action and Milestones                                 | The organization:  | Functional     | Intersects With   | Capabilities Deficiency Tracking                                | IAO-05   | Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification; and; (6) Remediation completion date, if applicable. | 5                        |       |

| FDE #     | FDE Name                                       | Focal Document Element (FDE) Description  | STRM Rationale | STRM Relationship | SCF Control   | SCF #    | Secure Controls Framework (SCF) Control Description   | Strength of Relationship | Notes                     |
|-----------|--|---|----------------|-------------------|---|----------|---|--------------------------|---------------------------|
| CA-5.a    | Plan of Action and Milestones                  | Develops and submits a plan of action and milestones (POA&M) for the information system within thirty (30) days of the final results for every internal/external audit/review or test (e.g., security controls assessment, penetration test) to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; | Functional     | Subset Of         | Capabilities Deficiency Tracking                                      | IAO-05   | Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency;(4) Risk associated with the deficiency;(5) Source deficiency identification/detection;(6) Temporary compensating controls, if applicable;(7) Point of Contact (POC) (e.g., asset/process owner);(8) Resources required to conduct remediation actions;(9) Planned remedial actions to the | 10                       |                           |
| CA-5.b    | Plan of Action and Milestones                  | Updates and submits the existing POA&M monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities; and  | Functional     | Subset Of         | Capabilities Deficiency Tracking                                      | IAO-05   | Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency;(4) Risk associated with the deficiency;(5) Source deficiency identification/detection;(6) Temporary compensating controls, if applicable;(7) Point of Contact (POC) (e.g., asset/process owner);(8) Resources required to conduct remediation actions;(9) Planned remedial actions to the | 10                       |                           |
| CA-5.c    | Plan of Action and Milestones                  | Submits an updated POA&M to CMS every three (3) months.   | Functional     | Subset Of         | Capabilities Deficiency Tracking                                      | IAO-05   | Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency;(4) Risk associated with the deficiency;(5) Source deficiency identification/detection;(6) Temporary compensating controls, if applicable;(7) Point of Contact (POC) (e.g., asset/process owner);(8) Resources required to conduct remediation actions;(9) Planned remedial actions to the | 10                       |                           |
| CA-5-1.1  | Plan of Action and Milestones                  | The Plan of Action and Milestones template is to be used for reporting POA&Ms to CMS and is found at: <a href="https://calt.cms.gov/projects/cms_aca_program_security_privacy/">https://calt.cms.gov/projects/cms_aca_program_security_privacy/</a> .   | Functional     | Subset Of         | Capabilities Deficiency Tracking                                      | IAO-05   | Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency;(4) Risk associated with the deficiency;(5) Source deficiency identification/detection;(6) Temporary compensating controls, if applicable;(7) Point of Contact (POC) (e.g., asset/process owner);(8) Resources required to conduct remediation actions;(9) Planned remedial actions to the | 10                       |                           |
| CA-5(1)   | Automation Support for Accuracy/Currency       | The organization employs automated mechanisms to help ensure that the plan of action and milestones for the information system is accurate, up to date, and readily available.  | Functional     | Subset Of         | Deficiency Tracking Automation  | IAO-05.1 | Mechanisms exist to help ensure tracked deficiencies are:(1) Accurate;(2) Up-to-date; and(3) Resilient-avoidable.   | 10                       |                           |
| CA-6      | Security Authorization                         | The organization:   | Functional     | Subset Of         | Security Authorization  | IAO-07   | Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.   | 10                       |                           |
| CA-6.a    | Security Authorization                         | Ensures that the Administering Entity (AE) authorizing official authorizes the information system for processing before commencing operations; and  | Functional     | Subset Of         | Security Authorization  | IAO-07   | Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.   | 10                       |                           |
| CA-6.b    | Security Authorization                         | Updates the security authorization:   | Functional     | Subset Of         | Security Authorization  | IAO-07   | Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.   | 10                       |                           |
| CA-6.b.1  | Security Authorization                         | Within every three (3) years;   | Functional     | Subset Of         | Security Authorization  | IAO-07   | Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.   | 10                       |                           |
| CA-6.b.2  | Security Authorization                         | When significant changes are made to the system;  | Functional     | Subset Of         | Security Authorization  | IAO-07   | Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.   | 10                       |                           |
| CA-6.b.3  | Security Authorization                         | When changes in requirements result in the need to process data of a higher sensitivity;  | Functional     | Subset Of         | Security Authorization  | IAO-07   | Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.   | 10                       |                           |
| CA-6.b.4  | Security Authorization                         | When changes occur to authorizing legislation or federal requirements;  | Functional     | Subset Of         | Security Authorization  | IAO-07   | Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.   | 10                       |                           |
| CA-6.b.5  | Security Authorization                         | After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and  | Functional     | Subset Of         | Security Authorization  | IAO-07   | Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.   | 10                       |                           |
| CA-6.b.6  | Security Authorization                         | Prior to expiration of a previous security authorization.   | Functional     | Subset Of         | Security Authorization  | IAO-07   | Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.   | 10                       |                           |
| CA-6.c    | Security Authorization                         | If the organization maintains a system-to-system connection with CMS through an escalated interconnection security agreement (ISA), the CMS-granted Authority to Connect (ATC) is updated:  | Functional     | Subset Of         | Security Authorization  | IAO-07   | Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.   | 10                       |                           |
| CA-6.c.1  | Security Authorization                         | Within every three (3) years;   | Functional     | Subset Of         | Security Authorization  | IAO-07   | Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.   | 10                       |                           |
| CA-6.c.2  | Security Authorization                         | When significant changes are made to the system;  | Functional     | Subset Of         | Security Authorization  | IAO-07   | Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.   | 10                       |                           |
| CA-6.c.3  | Security Authorization                         | When changes in requirements result in the need to process data of a higher sensitivity;  | Functional     | Subset Of         | Security Authorization  | IAO-07   | Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.   | 10                       |                           |
| CA-6.c.4  | Security Authorization                         | When changes occur to authorizing legislation or federal requirements;  | Functional     | Subset Of         | Security Authorization  | IAO-07   | Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.   | 10                       |                           |
| CA-6.c.5  | Security Authorization                         | After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and  | Functional     | Subset Of         | Security Authorization  | IAO-07   | Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.   | 10                       |                           |
| CA-6.c.6  | Security Authorization                         | Prior to expiration of a previous security authorization.   | Functional     | Subset Of         | 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-7      | Continuous Monitoring                          | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:  | Functional     | Subset Of         | Security, Compliance & Resilience Controls Oversight                  | CPL-02   | Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.  | 10                       |                           |
| CA-7.1    | Continuous Monitoring                          | Establishment of organizationally defined metrics (defined in the applicable security plan) to be monitored annually, at a minimum;   | Functional     | Subset Of         | Security, Compliance & Resilience Controls Oversight                  | CPL-02   | Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.  | 10                       |                           |
| CA-7.2    | Continuous Monitoring                          | Establishment of defined frequencies (defined in the applicable security plan) for monitoring and defined frequencies (defined in the applicable security plan) for assessments supporting such monitoring;   | Functional     | Subset Of         | Security, Compliance & Resilience Controls Oversight                  | CPL-02   | Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.  | 10                       |                           |
| CA-7.3    | Continuous Monitoring                          | Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;  | Functional     | Subset Of         | Security, Compliance & Resilience Controls Oversight                  | CPL-02   | Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.  | 10                       |                           |
| CA-7.4    | Continuous Monitoring                          | Ongoing security status monitoring of organizationally defined metrics in accordance with the organizational continuous monitoring strategy;  | Functional     | Subset Of         | Security, Compliance & Resilience Controls Oversight                  | CPL-02   | Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.  | 10                       |                           |
| CA-7.5    | Continuous Monitoring                          | Correlation and analysis of security-related information generated by assessments and monitoring;   | Functional     | Subset Of         | Security, Compliance & Resilience Controls Oversight                  | CPL-02   | Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.  | 10                       |                           |
| CA-7.6    | Continuous Monitoring                          | Response actions to address results of the analysis of security-related information;  | Functional     | Subset Of         | Security, Compliance & Resilience Controls Oversight                  | CPL-02   | Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.  | 10                       |                           |
| CA-7.7    | Continuous Monitoring                          | Reporting the security status of organization and the information system to defined personnel or roles (defined in the applicable security plan) monthly; and   | Functional     | Subset Of         | Security, Compliance & Resilience Controls Oversight                  | CPL-02   | Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.  | 10                       |                           |
| CA-7.8    | Continuous Monitoring                          | Reporting the security status of AE systems to defined personnel or roles (defined in the applicable security plan) at organizational-defined frequency, and reporting to CMS as specified in the Implementation Standard.  | Functional     | Subset Of         | Security, Compliance & Resilience Controls Oversight                  | CPL-02   | Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.  | 10                       |                           |
| CA-7-15   | Continuous Monitoring                          | CMS has specified continuous monitoring and reporting requirements for AE systems in operation in the Security and Privacy Oversight and Monitoring Guide for Administering Entity Systems in Operation, found at <a href="https://calt.cms.gov/projects/cms_aca_program_security_privacy/">https://calt.cms.gov/projects/cms_aca_program_security_privacy/</a> . Reporting requirements include:   | Functional     | Subset Of         | Security, Compliance & Resilience Controls Oversight                  | CPL-02   | Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.  | 10                       |                           |
| CA-7-15.1 | Continuous Monitoring                          | Quarterly reporting of Plans of Action & Milestones (POA&M)   | Functional     | Subset Of         | Security, Compliance & Resilience Controls Oversight                  | CPL-02   | Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.  | 10                       |                           |
| CA-7-15.2 | Continuous Monitoring                          | Annual Security Attestation   | Functional     | Subset Of         | Declaration of Conformity   | CPL-01.5 | Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document:(1) Is concise;(2) Unambiguously reflects the current status;(3) Is physically or electronically signed; and(4) Where possible, is machine readable.  | 10                       |                           |
| CA-7-15.2 | Continuous Monitoring                          | Annual Security Attestation   | Functional     | Subset Of         | Security, Compliance & Resilience Controls Oversight                  | CPL-02   | Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.  | 10                       |                           |
| CA-7-15.3 | Continuous Monitoring                          | Reporting of significant changes to the AE system   | Functional     | Subset Of         | Security, Compliance & Resilience Controls Oversight                  | CPL-02   | Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.  | 10                       |                           |
| CA-7(1)   | Independent Assessment                         | The use of independent security assessment agents or teams to monitor security controls is not required; however, if the organization employs assessors or assessment teams with CMS-defined level of independence to monitor the security controls in the information system on an ongoing basis, this can be used to satisfy security control assessment requirements.  | Functional     | Intersects With   | Independent Assessors   | CPL-03.1 | Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.   | 5                        |                           |
| CA-7(1)   | Independent Assessment                         | The use of independent security assessment agents or teams to monitor security controls is not required; however, if the organization employs assessors or assessment teams with CMS-defined level of independence to monitor the security controls in the information system on an ongoing basis, this can be used to satisfy security control assessment requirements.  | Functional     | Intersects With   | Security, Compliance & Resilience Controls Oversight                  | CPL-02   | Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.  | 5                        |                           |
| CA-9      | Internal System Connections                    | The organization:   | Functional     | Subset Of         | 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-9.a    | Internal System Connections                    | Authorizes connections of defined internal information system components or classes of components (defined in the applicable security plan) to the information system; and  | Functional     | Subset Of         | 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-9.b    | Internal System Connections                    | Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.  | Functional     | Subset Of         | 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                       |                           |
| 1.5       | Configuration Management (CM)                  | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A   | 0                        | No applicable SCF control |
| CM-1      | Configuration Management Policy and Procedures | The organization develops, documents, disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days;   | Functional     | Subset Of         | Configuration Management Program                                      | CFG-01   | Mechanisms exist to facilitate the implementation of configuration management controls.   | 10                       |                           |
| CM-1      | Configuration Management Policy and Procedures | The organization develops, documents, disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days;   | Functional     | Intersects With   | Periodic Review & Update of Security, Compliance & Resilience Program | GOV-03   | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.   | 5                        |                           |
| CM-1      | Configuration Management Policy and Procedures | The organization develops, documents, disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days;   | Functional     | Intersects With   | Publishing Security, Compliance & Resilience Documentation            | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.  | 5                        |                           |
| CM-1.a    | Configuration Management Policy and Procedures | A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and   | Functional     | Subset Of         | Publishing Security, Compliance & Resilience Documentation            | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.  | 10                       |                           |
| CM-1.b    | Configuration Management Policy and Procedures | Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.   | Functional     | Subset Of         | Standardized Operating Procedures (SOP)                               | OPS-01.1 | Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.   | 10                       |                           |
| CM-1.5    | Configuration Management Policy and Procedures | The organization documents the configuration management process and procedures to:  | Functional     | Subset Of         | Configuration Management Program                                      | CFG-01   | Mechanisms exist to facilitate the implementation of configuration management controls.   | 10                       |                           |

| FDE #        | FDE Name                                       | Focal Document Element (FDE) Description  | STRM Rationale | STRM Relationship | SCF Control   | SCF #    | Secure Controls Framework (SCF) Control Description   | Strength of Relationship | Notes |
|--------------|--|---|----------------|-------------------|---|----------|---|--------------------------|-------|
| CM-1-IS.1    | Configuration Management Policy and Procedures | Define configuration items at the system and component level (e.g., hardware, software, and workstation).   | Functional     | Subset Of         | Configuration Management Program                                | CFG-01   | Mechanisms exist to facilitate the implementation of configuration management controls.   | 10                       |       |
| CM-1-IS.2    | Configuration Management Policy and Procedures | Monitor configurations; and   | 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 technologies.  | 5                        |       |
| CM-1-IS.3    | Configuration Management Policy and Procedures | Track and approve changes prior to implementation, including but not limited to, flaw remediation, security patches, and emergency changes (e.g., unscheduled changes such as mitigating newly discovered security vulnerabilities, system crashes, and replacement of critical hardware components).   | Functional     | Subset Of         | Configuration Change Control                                    | CHG-02   | Mechanisms exist to govern the technical configuration change control processes.  | 10                       |       |
| CM-2         | Baseline Configuration                         | The organization develops, documents, and maintains under configuration control a current baseline configuration of the information system.   | 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-2         | Baseline Configuration                         | The organization develops, documents, and maintains under configuration control a current baseline configuration of the information system.   | Functional     | Intersects With   | Secure Baseline Configurations                                  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 5                        |       |
| CM-2(1)      | Reviews and Updates                            | The organization reviews and updates the baseline configuration of the information system.  | Functional     | Subset Of         | 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.  | 10                       |       |
| CM-2(1).a    | Reviews and Updates                            | At least every three hundred sixty-five (365) days.   | Functional     | Subset Of         | 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.  | 10                       |       |
| CM-2(1).b    | Reviews and Updates                            | When configuration settings change due to critical security patches, upgrades and emergency changes (e.g., unscheduled changes, system crashes, and replacement of critical hardware components), and major system changes/upgrades.  | Functional     | Subset Of         | 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.  | 10                       |       |
| CM-2(1).c    | Reviews and Updates                            | As an integral part of information system component installations, upgrades, and updates to applicable governing standards (implemented within the 365 days specified in number 1 above); and   | Functional     | Subset Of         | 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.  | 10                       |       |
| CM-2(1).d    | Reviews and Updates                            | Supporting baseline configuration documentation reflects ongoing implementation of operational configuration baseline updates, either directly or by policy.  | Functional     | Subset Of         | 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.  | 10                       |       |
| CM-2(1)-IS   | Reviews and Updates                            | The Service Provider reviews and updates the baseline configuration of the information system.  | Functional     | Subset Of         | Review of Third-Party Services                                  | TPM-08   | Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.   | 10                       |       |
| CM-2(1)-IS.1 | Reviews and Updates                            | Annually;   | Functional     | Subset Of         | Review of Third-Party Services                                  | TPM-08   | Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.   | 10                       |       |
| CM-2(1)-IS.2 | Reviews and Updates                            | When required due to a significant change; and  | Functional     | Subset Of         | Review of Third-Party Services                                  | TPM-08   | Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.   | 10                       |       |
| CM-2(1)-IS.3 | Reviews and Updates                            | As an integral part of information system component installations and upgrades.   | Functional     | Subset Of         | Review of Third-Party Services                                  | TPM-08   | Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.   | 10                       |       |
| CM-2(3)      | Retention of Previous Configurations           | The organization retains older versions of baseline configurations of the information system as deemed necessary to support rollback.   | Functional     | Subset Of         | Retention Of Previous Configurations                            | CFG-02.3 | Mechanisms exist to retain previous versions of baseline configuration to support roll back.  | 10                       |       |
| CM-3         | Configuration Change Control                   | The organization:   | Functional     | Subset Of         | Change Management Program                                       | CHG-01   | Mechanisms exist to facilitate the implementation of a change management program.   | 10                       |       |
| CM-3.a       | Configuration Change Control                   | Determines the types of changes to the information system that are configuration-controlled.  | Functional     | Intersects With   | Configuration Change Control                                    | CHG-02   | Mechanisms exist to govern the technical configuration change control processes.  | 5                        |       |
| CM-3.b       | Configuration Change Control                   | Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses.  | Functional     | Subset Of         | Configuration Change Control                                    | CHG-02   | Mechanisms exist to govern the technical configuration change control processes.  | 10                       |       |
| CM-3.c       | Configuration Change Control                   | Documents configuration change decisions associated with the information system.  | Functional     | Subset Of         | Configuration Change Control                                    | CHG-02   | Mechanisms exist to govern the technical configuration change control processes.  | 10                       |       |
| CM-3.d       | Configuration Change Control                   | Implements approved configuration-controlled changes to the information system.   | Functional     | Subset Of         | Configuration Change Control                                    | CHG-02   | Mechanisms exist to govern the technical configuration change control processes.  | 10                       |       |
| CM-3.e       | Configuration Change Control                   | Retains records of configuration-controlled changes to the information system for at least three (3) years.   | Functional     | Subset Of         | Change Management Program                                       | CHG-01   | Mechanisms exist to facilitate the implementation of a change management program.   | 10                       |       |
| CM-3.e       | Configuration Change Control                   | Retains records of configuration-controlled changes to the information system for at least three (3) years.   | Functional     | Subset Of         | Media & Data Retention  | DCH-18   | Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.  | 10                       |       |
| CM-3.f       | Configuration Change Control                   | Audits and reviews activities associated with configuration-controlled changes to the information system.   | Functional     | Subset Of         | Change Management Program                                       | CHG-01   | Mechanisms exist to facilitate the implementation of a change management program.   | 10                       |       |
| CM-3.g       | Configuration Change Control                   | Coordinates and provides oversight for configuration change control activities through change request forms that must be approved by an organizational and/or change control board that conveys frequently enough to accommodate proposed change requests, and by other appropriate organization officials including, but not limited to, the System Developer/Maintainer and information system support staff.   | Functional     | Subset Of         | Change Management Program                                       | CHG-01   | Mechanisms exist to facilitate the implementation of a change management program.   | 10                       |       |
| CM-3-IS.1    | Configuration Change Control                   | The system owner coordinates and provides oversight for configuration change control activities through organization-defined configuration change control processes (e.g., electronic bulletin board, or web status page). The means of communication are approved and accepted by the system owner. The means of communication with CMS about significant changes must follow the Change Reporting Procedures for State-Based Administering Entry Systems established by CMS, which can be found at: <a href="https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/">https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/</a> .   | Functional     | Subset Of         | Configuration Change Control                                    | CHG-02   | Mechanisms exist to govern the technical configuration change control processes.  | 10                       |       |
| CM-3-IS.2    | Configuration Change Control                   | The system owner defines the configuration change control element and the frequency or conditions under which it is covered.  | Functional     | Subset Of         | Configuration Change Control                                    | CHG-02   | Mechanisms exist to govern the technical configuration change control processes.  | 10                       |       |
| CM-3-IS.3    | Configuration Change Control                   | The organization establishes a central means of communicating significant changes to or developments in the information system or environment of operations that may affect its business agreements/contracts with CMS and business partners, and services to the business owner and associated service consumers (e.g., electronic bulletin board, or web status page). The means of communication are approved and accepted by the system owner. The means of communication with CMS about significant changes must follow the Change Reporting Procedures for State-Based Administering Entry Systems established by CMS, which can be found at: <a href="https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/">https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/</a> . | 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-3-IS.4    | Configuration Change Control                   | In establishing contracts with non-Exchange entities, the organization requires the non-Exchange entity to inform the organization of any changes in its administrative, technical, or operational environment defined as material within the contract.   | Functional     | Subset Of         | Third-Party Contract Requirements                               | TPM-05   | Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).                | 10                       |       |
| CM-3(2)      | Test/Validate/Document Changes                 | The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.   | Functional     | Intersects With   | Control Functionality Verification                              | CHG-06   | Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.   | 5                        |       |
| CM-3(2)      | Test/Validate/Document Changes                 | The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.   | Functional     | Intersects With   | Test, Validate & Document Changes                               | CHG-02.2 | Mechanisms exist to appropriately test and document proposed changes in a production environment.   | 5                        |       |
| CM-4         | Security Impact Analysis                       | The organization analyzes changes to the information system to determine potential security and privacy impacts prior to change implementation. Activities associated with configuration changes to the information system are audited.   | Functional     | Subset Of         | 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-4-IS.1    | Security Impact Analysis                       | A security impact analysis report is required as part of change reporting to CMS. The Change Reporting Procedures for State-Based Administering Entry Systems established by CMS can be found at: <a href="https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/">https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/</a> .   | Functional     | Subset Of         | 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-4(1)      | Separate Test Environments                     | The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibilities, or intentional malice. Processing or storing of Personally Identifiable Information (PII) in test environments is prohibited.   | Functional     | Subset Of         | 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-4(2)      | Verification of Security Functions             | The organization checks the security functions after the information system is changed to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome for meeting the system's security requirements.   | Functional     | Subset Of         | Technical Verification  | IAO-06   | Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.  | 10                       |       |
| CM-5         | Access Restrictions for Change                 | The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Records reflecting all such changes shall be generated, reviewed, and retained.   | 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-5         | Access Restrictions for Change                 | The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Records reflecting all such changes shall be generated, reviewed, and retained.   | 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-5(1)      | Automated Access Enforcement/Auditing          | The organization employs automated mechanisms to enforce access restrictions to configuration change information and support auditing of the enforcement actions.   | Functional     | Subset Of         | 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-5(5)      | Limit Production/Operational Privileges        | The organization:   | Functional     | Subset Of         | Permissions To Implement Changes                                | CHG-04.4 | Mechanisms exist to limit operational privileges for implementing changes.  | 10                       |       |
| CM-5(5).a    | Limit Production/Operational Privileges        | Limits privileges to change information system components and system-related information with in a production or operational environment; and   | Functional     | Subset Of         | Permissions To Implement Changes                                | CHG-04.4 | Mechanisms exist to limit operational privileges for implementing changes.  | 10                       |       |
| CM-5(5).b    | Limit Production/Operational Privileges        | Reviews and reevaluates privileges at least quarterly.  | Functional     | Subset Of         | Permissions To Implement Changes                                | CHG-04.4 | Mechanisms exist to limit operational privileges for implementing changes.  | 5                        |       |
| CM-6         | Configuration Settings                         | The organization:   | Functional     | Intersects With   | Secure Baseline Configurations                                  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 5                        |       |
| CM-6         | Configuration Settings                         | The organization:   | Functional     | Intersects With   | Approved Configuration Deviations                               | CFG-02.7 | Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.  | 5                        |       |
| CM-6.a       | Configuration Settings                         | Establishes and documents mandatory configuration settings for information technology products employed within the information system using the latest security configuration guidelines listed in Implementation Standard 1 that reflect the most restrictive mode consistent with operational requirements.   | Functional     | Subset Of         | Secure Baseline Configurations                                  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| CM-6.b       | Configuration Settings                         | Implements the configuration settings;  | Functional     | Subset Of         | Secure Baseline Configurations                                  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| CM-6.c       | Configuration Settings                         | Identifies, documents, and approves any deviations from established configuration settings for individual components within the information system based on explicit operational requirements; and  | Functional     | Subset Of         | Approved Configuration Deviations                               | CFG-02.7 | Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.  | 10                       |       |

| FDE #       | FDE Name   | Focal Document Element (FDE) Description   | STRM Rationale | STRM Relationship | SCF Control                                 | SCF #    | Secure Controls Framework (SCF) Control Description   | Strength of Relationship | Notes |
|-------------|--|--|----------------|-------------------|---|----------|---|--------------------------|-------|
| CM-6.d      | Configuration Settings                                 | Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.   | 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 technologies.  | 5                        |       |
| CM-6-IS.1   | Configuration Settings                                 | Security configuration guidelines may be developed by different federal agencies. Therefore, it is possible that a guideline could include configuration information that conflicts with another agency or the organization's guideline. To resolve configuration conflicts among multiple security guidelines, the organization's hierarchy for implementing all security configuration guidelines is as follows: | Functional     | Subset Of         | Baseline Tailoring                          | CFG-02.9 | Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to:(1) Mission / business functions;(2) Operational environment;(3) Specific threats or vulnerabilities; or(4) Other conditions or situations that could affect mission / business success.  | 10                       |       |
| CM-6-IS.1.a | Configuration Settings                                 | National Institute of Standards and Technology (NIST)  | Functional     | Subset Of         | Baseline Tailoring                          | CFG-02.9 | Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to:(1) Mission / business functions;(2) Operational environment;(3) Specific threats or vulnerabilities; or(4) Other conditions or situations that could affect mission / business success.  | 10                       |       |
| CM-6-IS.1.b | Configuration Settings                                 | CMS  | Functional     | Subset Of         | Baseline Tailoring                          | CFG-02.9 | Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to:(1) Mission / business functions;(2) Operational environment;(3) Specific threats or vulnerabilities; or(4) Other conditions or situations that could affect mission / business success.  | 10                       |       |
| CM-6-IS.1.c | Configuration Settings                                 | Defense Information Systems Agency (DISA)  | Functional     | Subset Of         | Baseline Tailoring                          | CFG-02.9 | Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to:(1) Mission / business functions;(2) Operational environment;(3) Specific threats or vulnerabilities; or(4) Other conditions or situations that could affect mission / business success.  | 10                       |       |
| CM-6-IS.1.d | Configuration Settings                                 | Office of Management and Budget (OMB)  | Functional     | Subset Of         | Baseline Tailoring                          | CFG-02.9 | Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to:(1) Mission / business functions;(2) Operational environment;(3) Specific threats or vulnerabilities; or(4) Other conditions or situations that could affect mission / business success.  | 10                       |       |
| CM-6-IS.2   | Configuration Settings                                 | If formal government-authored checklists do not exist, then organizations are encouraged to use vendor or industry group, such as The Center for Internet Security (CIS) checklists.   | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| CM-6-IS.3   | Configuration Settings                                 | The organization ensures that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available).  | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| CM-6(I)     | Automated Central Management/ Application/Verification | The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for information technology products.   | 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 technologies.  | 5                        |       |
| CM-7        | Least Functionality                                    | The organization:  | Functional     | Subset Of         | 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-7.a      | Least Functionality                                    | Configures the information system to provide only essential capabilities; and  | Functional     | Subset Of         | 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-7.b      | Least Functionality                                    | Prohibits or restricts the use of high-risk system services, ports, network protocols, and capabilities (e.g., Telnet/FTP, etc.) across network boundaries that are not explicitly required for system or application functionality. A list of specifically needed system services, ports, and network protocols will be maintained and documented in the applicable security plan; all others will be disabled.   | Functional     | Subset Of         | 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-7-IS.1   | Least Functionality                                    | The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: United States Government Configuration Baseline (USGCB)-defined list of prohibited or restricted functions, ports, protocols, and/or services.  | Functional     | Subset Of         | 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-7-IS.2   | Least Functionality                                    | The organization shall use the Center for Internet Security guidelines (Level 1) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if USGCB is not available.  | Functional     | Subset Of         | Secure Baseline Configurations              | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |       |
| CM-7(1)     | Periodic Review  | The organization:  | Functional     | Subset Of         | Periodic Review                             | CFG-03.1 | Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.   | 10                       |       |
| CM-7(1).a   | Periodic Review  | Reviews the information system at least quarterly to identify and eliminate unnecessary functions, ports, protocols, and/or services; and  | Functional     | Subset Of         | Periodic Review                             | CFG-03.1 | Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.   | 10                       |       |
| CM-7(1).b   | Periodic Review  | Disables functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.   | Functional     | Subset Of         | Periodic Review                             | CFG-03.1 | Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.   | 10                       |       |
| CM-7(2)     | Prevent Program Execution                              | The information system prevents program execution in accordance with the list of authorized or unauthorized software programs and 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-7(2)     | Prevent Program Execution                              | The information system prevents program execution in accordance with the list of authorized or unauthorized software programs and 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-7(4)     | Unauthorized Software/Blacklisting                     | The organization:  | Functional     | Subset Of         | Explicitly Allow / Deny Applications        | CFG-03.3 | Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.  | 10                       |       |
| CM-7(4).a   | Unauthorized Software/Blacklisting                     | Identifies defined software programs (defined in the applicable security plan) not authorized to execute on the information system;  | Functional     | Subset Of         | Explicitly Allow / Deny Applications        | CFG-03.3 | Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.  | 10                       |       |
| CM-7(4).b   | Unauthorized Software/Blacklisting                     | Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and  | Functional     | Subset Of         | Explicitly Allow / Deny Applications        | CFG-03.3 | Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.  | 10                       |       |
| CM-7(4).c   | Unauthorized Software/Blacklisting                     | Reviews and updates the list of unauthorized software programs within every three hundred sixty-five (365) days.   | Functional     | Subset Of         | 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-8        | Information System Component Inventory                 | The organization:  | Functional     | Subset Of         | 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. | 10                       |       |
| CM-8        | Information System Component Inventory                 | The organization:  | Functional     | Intersects With   | Component Duplication Avoidance             | AST-02.3 | Mechanisms exist to establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components that prevents assets from being duplicated in other asset inventories.  | 5                        |       |
| CM-8.a      | Information System Component Inventory                 | Develops and documents an inventory of information system components that:   | Functional     | Subset Of         | 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. | 10                       |       |
| CM-8.a.1    | Information System Component Inventory                 | Accurately reflects the current information system;  | Functional     | Subset Of         | 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. | 10                       |       |
| CM-8.a.2    | Information System Component Inventory                 | Includes all components within the authorization boundary of the information system;   | Functional     | Subset Of         | 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. | 10                       |       |
| CM-8.a.3    | Information System Component Inventory                 | Is at the level of granularity deemed necessary for tracking and reporting; and  | Functional     | Subset Of         | 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. | 10                       |       |

| FDE #        | FDE Name                                   | Focal Document Element (FDE) Description   | STRM Rationale | STRM Relationship | SCF Control   | SCF #    | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes                     |
|--------------|--|--|----------------|-------------------|---|----------|--|--------------------------|---------------------------|
| CM-8.a.4     | Information System Component Inventory     | Includes: organization-defined information deemed necessary to achieve effective property accountability, which may include hardware inventory specifications (e.g., manufacturer, type, model, serial number, and physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address. | Functional     | Subset Of         | 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. | 10                       |                           |
| CM-8.b       | Information System Component Inventory     | Reviews and updates the information system component inventory no less than every three hundred sixty-five (365) days, or per CM-8 (1) and/or CM-8 (2), as applicable.   | Functional     | Subset Of         | 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. | 10                       |                           |
| CM-8-IS.1    | Information System Component Inventory     | The organization defines information deemed necessary to achieve effective property accountability.  | Functional     | Subset Of         | 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. | 10                       |                           |
| CM-8-IS.2    | Information System Component Inventory     | The organization establishes, maintains, and updates, within every three hundred sixty-five (365) days, an inventory that includes a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII).   | Functional     | Subset Of         | 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. | 10                       |                           |
| CM-8(1)      | Updates During Installations/Removals      | The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.  | Functional     | Subset Of         | Updates During Installations / Removals                               | AST-02.1 | Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades.  | 10                       |                           |
| CM-8(3)      | Automated Unauthorized Component Detection | The organization:  | Functional     | Subset Of         | Automated Unauthorized Component Detection                            | AST-02.2 | Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.  | 10                       |                           |
| CM-8(3)      | Automated Unauthorized Component Detection | The organization:  | Functional     | Intersects With   | Software Installation Alerts  | END-03.1 | Mechanisms exist to generate an alert when new software is detected.   | 5                        |                           |
| CM-8(3)      | Automated Unauthorized Component Detection | The organization:  | Functional     | Intersects With   | Unauthorized Installation Alerts                                      | CFG-05.1 | Mechanisms exist to generate an alert when the unauthorized installation of software is detected.  | 5                        |                           |
| CM-8(3).a    | Automated Unauthorized Component Detection | Employs automated mechanisms to scan the network no less than weekly to detect the presence of unauthorized hardware, software, and firmware components within the information system; and   | Functional     | Subset Of         | Automated Unauthorized Component Detection                            | AST-02.2 | Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.  | 10                       |                           |
| CM-8(3).b    | Automated Unauthorized Component Detection | Takes the following actions when unauthorized components are detected: disables network access by such components/devices and notifies defined personnel or roles (defined in the applicable security plan).   | Functional     | Subset Of         | Automated Unauthorized Component Detection                            | AST-02.2 | Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.  | 10                       |                           |
| CM-8(3)-IS   | Automated Unauthorized Component Detection | In a shared computing facility, the Service Provider:  | Functional     | Subset Of         | Automated Unauthorized Component Detection                            | AST-02.2 | Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.  | 10                       |                           |
| CM-8(3)-IS.1 | Automated Unauthorized Component Detection | Employs automated mechanisms to scan continuously, using automated mechanisms with a maximum (5) five-minute delay in detection to detect the addition of unauthorized components/devices into the information system; and   | Functional     | Subset Of         | Automated Unauthorized Component Detection                            | AST-02.2 | Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.  | 10                       |                           |
| CM-8(3)-IS.2 | Automated Unauthorized Component Detection | Disables network access by such components/devices or notifies designated organizational officials.  | Functional     | Subset Of         | Automated Unauthorized Component Detection                            | AST-02.2 | Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.  | 10                       |                           |
| CM-8(5)      | No Duplicate Accounting of Components      | The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.  | Functional     | Subset Of         | 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.   | 10                       |                           |
| CM-9         | Configuration Management Plan              | The organization develops, documents, and implements a configuration management plan for the information system that:  | Functional     | Subset Of         | Configuration Management Program                                      | CFG-01   | Mechanisms exist to facilitate the implementation of configuration management controls.  | 10                       |                           |
| CM-9         | Configuration Management Plan              | The organization develops, documents, and implements a configuration management plan for the information system that:  | 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-9.a       | Configuration Management Plan              | Addresses roles, responsibilities, and configuration management processes and procedures;  | Functional     | Subset Of         | Configuration Management Program                                      | CFG-01   | Mechanisms exist to facilitate the implementation of configuration management controls.  | 10                       |                           |
| CM-9.b       | Configuration Management Plan              | Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;  | Functional     | Subset Of         | Configuration Management Program                                      | CFG-01   | Mechanisms exist to facilitate the implementation of configuration management controls.  | 10                       |                           |
| CM-9.c       | Configuration Management Plan              | Defines the configuration items for the information system and places the configuration items under configuration management; and  | Functional     | Subset Of         | Configuration Management Program                                      | CFG-01   | Mechanisms exist to facilitate the implementation of configuration management controls.  | 10                       |                           |
| CM-9.d       | Configuration Management Plan              | Protects the configuration management plan from unauthorized disclosure and modification.  | Functional     | Subset Of         | Configuration Management Program                                      | CFG-01   | Mechanisms exist to facilitate the implementation of configuration management controls.  | 10                       |                           |
| CM-10        | Software Usage Restrictions                | The organization:  | Functional     | Subset Of         | Software Usage Restrictions   | CFG-04   | Mechanisms exist to enforce software usage restrictions to comply with applicable contract agreements and copyright laws.  | 10                       |                           |
| CM-10.a      | Software Usage Restrictions                | Uses software and associated documentation in accordance with contract agreements and copyright laws;  | Functional     | Subset Of         | Software Usage Restrictions   | CFG-04   | Mechanisms exist to enforce software usage restrictions to comply with applicable contract agreements and copyright laws.  | 10                       |                           |
| CM-10.b      | Software Usage Restrictions                | Tracks the use of software and associated documentation protected by quantity specific contract copying and distribution laws;   | Functional     | Subset Of         | Software Usage Restrictions   | CFG-04   | Mechanisms exist to enforce software usage restrictions to comply with applicable contract agreements and copyright laws.  | 10                       |                           |
| CM-10.c      | Software Usage Restrictions                | Controls and documents 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 copyrighted work.  | Functional     | Subset Of         | Software Usage Restrictions   | CFG-04   | Mechanisms exist to enforce software usage restrictions to comply with applicable contract agreements and copyright laws.  | 10                       |                           |
| CM-10(1)     | Open Source Software                       | The organization establishes restrictions on the use of open source software. Open source software must:   | Functional     | Subset Of         | Open Source Software  | CFG-04.1 | Mechanisms exist to establish parameters for the secure use of open source software.   | 10                       |                           |
| CM-10(1).a   | Open Source Software                       | Be legally licensed;   | Functional     | Subset Of         | Open Source Software  | CFG-04.1 | Mechanisms exist to establish parameters for the secure use of open source software.   | 10                       |                           |
| CM-10(1).b   | Open Source Software                       | Approved by the agency information technology department; and  | Functional     | Subset Of         | Open Source Software  | CFG-04.1 | Mechanisms exist to establish parameters for the secure use of open source software.   | 10                       |                           |
| CM-10(1).c   | Open Source Software                       | Adhere to a secure configuration baseline checklist from the U.S. Government or industry.  | Functional     | Subset Of         | Open Source Software  | CFG-04.1 | Mechanisms exist to establish parameters for the secure use of open source software.   | 10                       |                           |
| CM-11        | User-Installed Software                    | The organization:  | Functional     | Intersects With   | Prohibit Installation Without Privileged Status                       | END-03   | Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.   | 5                        |                           |
| CM-11        | User-Installed Software                    | The organization:  | Functional     | Subset Of         | User-Installed Software   | CFG-05   | Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.   | 10                       |                           |
| CM-11.a      | User-Installed Software                    | Establishes organization-defined policies governing the installation of software by users;   | Functional     | Subset Of         | User-Installed Software   | CFG-05   | Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.   | 10                       |                           |
| CM-11.b      | User-Installed Software                    | Enforces software installation policies through organization-defined methods; and  | Functional     | Subset Of         | User-Installed Software   | CFG-05   | Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.   | 10                       |                           |
| CM-11.c      | User-Installed Software                    | Monitors policy compliance at organization-defined frequency.  | Functional     | Subset Of         | User-Installed Software   | CFG-05   | Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.   | 10                       |                           |
| 1.6          | Contingency Planning (CP)                  | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control |
| CP-1         | Contingency Planning Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:  | Functional     | Intersects With   | Periodic Review & Update of Security, Compliance & Resilience Program | GOV-03   | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.  | 5                        |                           |
| CP-1         | Contingency Planning Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:  | 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 (BCDR) playbooks).   | 10                       |                           |
| CP-1         | Contingency Planning Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:  | Functional     | Intersects With   | Publishing Security, Compliance & Resilience Documentation            | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.   | 5                        |                           |
| CP-1.a       | Contingency Planning Policy and Procedures | A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  | Functional     | Subset Of         | Publishing Security, Compliance & Resilience Documentation            | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.   | 10                       |                           |
| CP-1.b       | Contingency Planning Policy and Procedures | Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.  | Functional     | Subset Of         | Standardized Operating Procedures (SOP)                               | OPS-01.1 | Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to ensure the proper execution of day-to-day / assigned tasks.  | 10                       |                           |
| CP-2         | Contingency Plan                           | The organization:  | 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 (BCDR) playbooks).   | 10                       |                           |
| CP-2         | Contingency Plan                           | The organization:  | Functional     | Intersects With   | Business Continuity & Disaster Recovery (BCDR) Plans                  | BCD-01.7 | Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BCDR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.  | 5                        |                           |
| CP-2         | Contingency Plan                           | The organization:  | Functional     | Intersects With   | Ongoing Contingency Planning  | BCD-06   | Mechanisms exist to update contingency plans due to changes affecting: (1) People (e.g., personnel changes); (2) Processes (e.g., new, altered or decommissioned business practices, including third-party services); (3) Technology (e.g., hardware, software, or services); and (4) Other (e.g., changes in laws, regulations, or standards).  | 5                        |                           |
| CP-2.a       | Contingency Plan                           | Develops a contingency plan for the information system in accordance with NIST SP 800-34 that:   | Functional     | Intersects With   | Business Continuity & Disaster Recovery (BCDR) Plans                  | BCD-01.7 | Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BCDR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.  | 5                        |                           |
| CP-2.a.1     | Contingency Plan                           | Identifies essential organizational missions and business functions and associated contingency requirements;   | 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 (BCDR) playbooks).   | 10                       |                           |
| CP-2.a.2     | Contingency Plan                           | Provides recovery objectives, restoration priorities, and metrics;   | 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 (BCDR) playbooks).   | 10                       |                           |

| FDE #      | FDE Name                                     | Focal Document Element (FDE) Description  | STRM Rationale | STRM Relationship | SCF Control  | SCF #    | Secure Controls Framework (SCF) Control Description   | Strength of Relationship | Notes |
|------------|--|---|----------------|-------------------|--|----------|---|--------------------------|-------|
| CP-2.a.3   | Contingency Plan                             | Addresses contingency roles, responsibilities, assigned individuals with contact information.   | 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 (BCDR) playbooks).  | 10                       |       |
| CP-2.a.4   | Contingency Plan                             | Addresses maintaining essential organizational missions and business functions despite an information system disruption, compromise, or failure.  | 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 (BCDR) playbooks).  | 10                       |       |
| CP-2.a.5   | Contingency Plan                             | Addresses eventual, full information system restoration without deterioration of the security safeguards original planned and implemented; and  | 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 (BCDR) playbooks).  | 10                       |       |
| CP-2.a.6   | Contingency Plan                             | Is reviewed and approved by designated officials within the organization;   | 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 (BCDR) playbooks).  | 10                       |       |
| CP-2.b     | Contingency Plan                             | Distributes copies of the contingency plan to the Information System Security Officer, Business Owner, Contingency Plan Coordinator, CMS, and other stakeholders identified within the contingency plan;  | 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 (BCDR) playbooks).  | 10                       |       |
| CP-2.c     | Contingency Plan                             | Coordinates contingency planning activities with incident handling activities;  | 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 (BCDR) playbooks).  | 10                       |       |
| CP-2.d     | Contingency Plan                             | Reviews the contingency plan for the information system within every three hundred sixty-five (365) days;   | 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 (BCDR) playbooks).  | 10                       |       |
| CP-2.e     | Contingency Plan                             | Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.  | 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 (BCDR) playbooks).  | 10                       |       |
| CP-2.e     | Contingency Plan                             | Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;  | Functional     | Subset Of         | Ongoing Contingency Planning                                 | BCD-06   | Mechanisms exist to update contingency plans due to changes affecting:(1) People (e.g., personnel changes);(2) Processes (e.g., new, altered or decommissioned business practices, including third-party services);(3) Technologies (e.g., new, altered or decommissioned technologies);(4) Data (e.g., changes to data flows and/or data repositories);(5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or(6) Feedback from contingency plan testing activities. | 10                       |       |
| CP-2.f     | Contingency Plan                             | Communicates contingency plan changes to key contingency personnel and organizational elements identified above; and  | 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 (BCDR) playbooks).  | 10                       |       |
| CP-2.g     | Contingency Plan                             | Protects the contingency plan from unauthorized disclosure and modification.  | 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 (BCDR) playbooks).  | 10                       |       |
| CP-2.H.1   | Contingency Plan                             | The system owner defines a list of key contingency personnel (identified by name and/or role) and organizational elements for distribution and receipt of the contingency plan and any contingency plan changes. The contingency list includes designated CMS personnel.  | 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 (BCDR) playbooks).  | 10                       |       |
| CP-2(I)    | Coordinate with Related Plans                | The organization coordinates contingency plan development with organizational elements responsible for related plans.   | Functional     | Subset Of         | 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-2(J)    | Capacity Planning                            | The organization conducts capacity planning to ensure the necessary capacity for information processing, telecommunications, and environmental support during contingency operations.   | Functional     | Subset Of         | 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-2(K)    | Resume Essential Missions/Business Functions | The organization plans for the resumption of essential missions and business functions within the approved Maximum Tolerable Downtime (MTD), determined by the business owner, for the business functions.  | Functional     | Intersects With   | Resume All Missions & Business Functions                     | BCD-02.1 | Mechanisms exist to resume all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation.   | 5                        |       |
| CP-2(L)    | Identify Critical Assets                     | The organization identifies critical information system assets supporting essential missions and business functions.  | Functional     | Subset Of         | 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-3       | Contingency Training                         | The organization provides contingency training to operational and support personnel (including managers and information system users) consistent with assigned roles and responsibilities.  | Functional     | Subset Of         | Contingency Training   | BCD-03   | Mechanisms exist to adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities.   | 10                       |       |
| CP-3.a     | Contingency Training                         | Within ninety (90) days of assuming a contingency role or responsibility;   | Functional     | Subset Of         | Contingency Training   | BCD-03   | Mechanisms exist to adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities.   | 10                       |       |
| CP-3.b     | Contingency Training                         | When required by information system changes; and  | Functional     | Subset Of         | Contingency Training   | BCD-03   | Mechanisms exist to adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities.   | 10                       |       |
| CP-3.c     | Contingency Training                         | Within every three hundred sixty-five (365) days thereafter.  | Functional     | Subset Of         | Contingency Training   | BCD-03   | Mechanisms exist to adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities.   | 10                       |       |
| CP-4       | Contingency Plan Testing                     | The organization:   | Functional     | Intersects With   | Contingency Plan Root Cause Analysis (RCA) & Lessons Learned | BCD-05   | Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.  | 5                        |       |
| CP-4       | Contingency Plan Testing                     | The organization:   | Functional     | Subset Of         | 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.   | 10                       |       |
| CP-4.a     | Contingency Plan Testing                     | Tests the contingency plan for the information system within every three hundred sixty-five (365) days using functional exercises to determine the effectiveness of the plan and the organization's readiness to execute the plan;  | Functional     | Subset Of         | 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.   | 10                       |       |
| CP-4.b     | Contingency Plan Testing                     | Reviews the contingency plan test results; and  | Functional     | Subset Of         | 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.   | 10                       |       |
| CP-4.c     | Contingency Plan Testing                     | Initiates corrective actions, if needed   | Functional     | Subset Of         | 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.   | 10                       |       |
| CP-4.H.1   | Contingency Plan Testing                     | Must produce an after-action report to improve existing processes, procedures, and policies.  | Functional     | Subset Of         | 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.   | 10                       |       |
| CP-4(I)    | Coordinate with Related Plans                | The organization coordinates contingency plan testing with organizational elements responsible for related plans.   | Functional     | Subset Of         | 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-6       | Alternate Storage Site                       | The organization:   | Functional     | Subset Of         | Alternate Storage Site                                       | BCD-08   | Mechanisms exist to establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup information.   | 10                       |       |
| CP-6.a     | Alternate Storage Site                       | Establishes an alternate storage site as well as the necessary agreements to permit the storage and retrieval of information system backup information; and   | Functional     | Subset Of         | Alternate Storage Site                                       | BCD-08   | Mechanisms exist to establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup information.   | 10                       |       |
| CP-6.b     | Alternate Storage Site                       | Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.  | Functional     | Subset Of         | Alternate Storage Site                                       | BCD-08   | Mechanisms exist to establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup information.   | 10                       |       |
| CP-6(I)    | Separation from Primary Site                 | The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.   | Functional     | Subset Of         | Separation from Primary Storage Site                         | BCD-08.1 | Mechanisms exist to separate the alternate storage site from the primary storage site to reduce susceptibility to similar threats.  | 10                       |       |
| CP-6(J)    | Accessibility                                | The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.  | Functional     | Subset Of         | Primary Storage Site Accessibility                           | BCD-08.2 | Mechanisms exist to identify and mitigate potential accessibility problems to the alternate storage sites in the event of an area-wide disruption or disaster.  | 10                       |       |
| CP-7       | Alternate Processing Site                    | The organization:   | Functional     | Subset Of         | 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-7.a     | Alternate Processing Site                    | Establishes an alternate processing site as well as the necessary agreements to permit the transfer and resumption of information system operations for essential missions/business functions within the time period specified in Implementation Standard 1 when the primary processing capabilities are unavailable;   | Functional     | Subset Of         | 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-7.b     | Alternate Processing Site                    | Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and  | Functional     | Subset Of         | 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-7.c     | Alternate Processing Site                    | Ensures that the alternate processing site provides information security safeguards equivalent to those of the primary site.  | Functional     | Subset Of         | 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-7.H.1   | Alternate Processing Site                    | Ensure all equipment and supplies required for resuming system operations at the alternate processing site are available; or contracts are in place to support delivery to the site, to permit resumption of essential missions and business functions within a resumption time period consistent with the recovery time objectives defined by the business owner in the contingency plan.  | Functional     | Subset Of         | 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-7(I)    | Separation from Primary Site                 | The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.   | Functional     | Subset Of         | Separation from Primary Processing Site                      | BCD-09.1 | Mechanisms exist to separate the alternate processing site from the primary processing site to reduce susceptibility to similar threats.  | 10                       |       |
| CP-7(J)    | Accessibility                                | The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.   | Functional     | Subset Of         | Alternate Processing Site Accessibility                      | BCD-09.2 | Mechanisms exist to identify and mitigate potential accessibility problems to the alternate processing sites and possible mitigation actions, in the event of an area-wide disruption or disaster.  | 10                       |       |
| CP-7(K)    | Priority of Service                          | The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organizational availability requirements (including recovery time objectives).  | Functional     | Subset Of         | 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-8       | Telecommunications Services                  | The organization establishes alternate telecommunications services as well as the necessary agreements to permit the resumption of information system operations for essential organizational missions and business functions within the resumption time period specified in Implementation Standard 1 when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. | Functional     | Subset Of         | Telecommunications Services Availability                     | BCD-10   | Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services.  | 10                       |       |
| CP-8.H.1.a | Telecommunications Services                  | Ensure alternate telecommunications Service Level Agreements (SLA) are in place to permit resumption of system Recovery Time Objectives (RTO) and business function Maximum Tolerable Downtimes (MTD).  | Functional     | Subset Of         | Telecommunications Services Availability                     | BCD-10   | Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services.  | 10                       |       |
| CP-8.H.1.b | Telecommunications Services                  | The system owner defines a resumption time period consistent with the RTOs and business impact analysis. The time period is approved and accepted by the business owner.  | Functional     | Subset Of         | Telecommunications Services Availability                     | BCD-10   | Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services.  | 10                       |       |
| CP-8(I)    | Priority of Service Provisions               | N/A   | Functional     | Subset Of         | 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                       |       |

| FDE #       | FDE Name   | Focal Document Element (FDE) Description   | STRM Rationale | STRM Relationship | SCF Control  | SCF #    | Secure Controls Framework (SCF) Control Description   | Strength of Relationship | Notes                     |
|-------------|--|--|----------------|-------------------|--|----------|---|--------------------------|---------------------------|
| CP-8(1).a   | Priority of Service Provisions                           | Develops primary and alternate telecommunications service agreements that contain priority of service provisions in accordance with organizational availability requirements (including recovery time objectives); and   | Functional     | Subset Of         | 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-8(1).b   | Priority of Service Provisions                           | Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.  | Functional     | Subset Of         | 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-8(2)     | Single Points of Failure                                 | The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.   | Functional     | Intersects With   | Telecommunications Services Availability   | BCD-10   | Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services.  | 5                        |                           |
| CP-9        | Information System Backup                                | The organization:  | Functional     | Subset Of         | 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).  | 10                       |                           |
| CP-9.a      | Information System Backup                                | Conducts backups of user-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1;  | Functional     | Subset Of         | 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).  | 10                       |                           |
| CP-9.b      | Information System Backup                                | Conducts backups of system-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1;  | Functional     | Subset Of         | 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).  | 10                       |                           |
| CP-9.c      | Information System Backup                                | Conducts backups of information system documentation, including security-related documentation, other forms of data, and paper records, within the frequency defined in the applicable security plan, consistent with recovery time and recovery point objectives; and   | Functional     | Subset Of         | 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).  | 10                       |                           |
| CP-9.d      | Information System Backup                                | Protects the confidentiality, integrity, and availability of backup information at storage locations.  | Functional     | Subset Of         | 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).  | 10                       |                           |
| CP-9-1.1    | Information System Backup                                | Perform full backups weekly to separate media. Perform incremental or differential backups daily to separate media. Backups to include user-level and system-level information (including system state information). Three (3) generations of backups (full as well as all related incremental or differential backups) are stored off site. Off-site and on-site backups must be logged with name, date, time and action. | Functional     | Subset Of         | 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).  | 10                       |                           |
| CP-9-1.2    | Information System Backup                                | Ensure that a current, retrievable, copy of Personally Identifiable Information (PII) is available before movement of servers.   | Functional     | Subset Of         | 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).  | 10                       |                           |
| CP-9-1.3    | Information System Backup                                | Cloud environments The system owner shall determine what elements of the cloud environment require the Information System Backup control.  | Functional     | Subset Of         | 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).  | 10                       |                           |
| CP-9-1.4    | Information System Backup                                | Cloud environments The system owner determines how Information System Backup will be verified and the appropriate periodicity of the check.  | Functional     | Subset Of         | 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).  | 10                       |                           |
| CP-9(1)     | Testing for Reliability/Integrity                        | The organization tests backup information following each backup to verify media reliability and information integrity.   | Functional     | Subset Of         | Testing for Reliability & Integrity  | BCD-11.1 | Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.  | 10                       |                           |
| CP-9(1)-1.1 | Testing for Reliability/Integrity                        | The organization tests backup information at least annually.   | Functional     | Subset Of         | 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-10       | Information System Recovery and Reconstitution           | The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery of the information system after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.  | Functional     | Subset Of         | Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution | BCD-12   | Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.   | 10                       |                           |
| CP-10       | Information System Recovery and Reconstitution           | The organization provides for the recovery and reconstitution of the information system to a known state after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.   | 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 (COP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).  | 5                        |                           |
| CP-10       | Information System Recovery and Reconstitution           | The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery of the information system after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.  | 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-10-1.1   | Information System Recovery and Reconstitution           | Secure information system recovery and reconstitution includes, but is not limited to:   | Functional     | Subset Of         | Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution | BCD-12   | Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.   | 10                       |                           |
| CP-10-1.1.a | Information System Recovery and Reconstitution           | Reset all system parameters (either default or organization-established);  | Functional     | Subset Of         | Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution | BCD-12   | Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.   | 10                       |                           |
| CP-10-1.1.b | Information System Recovery and Reconstitution           | Reinstall patches;   | Functional     | Subset Of         | Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution | BCD-12   | Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.   | 10                       |                           |
| CP-10-1.1.c | Information System Recovery and Reconstitution           | Reestablish configuration settings;  | Functional     | Subset Of         | Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution | BCD-12   | Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.   | 10                       |                           |
| CP-10-1.1.c | Information System Recovery and Reconstitution           | Reestablish configuration settings;  | Functional     | Subset Of         | Secure Baseline Configurations   | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 10                       |                           |
| CP-10-1.1.d | Information System Recovery and Reconstitution           | Reinstall application and system software; and   | Functional     | Subset Of         | Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution | BCD-12   | Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.   | 10                       |                           |
| CP-10-1.1.e | Information System Recovery and Reconstitution           | Fully test the system.   | Functional     | Subset Of         | Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution | BCD-12   | Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.   | 10                       |                           |
| CP-10(2)    | Transaction Recovery                                     | The information system implements transaction recovery for transaction-based systems.  | Functional     | Intersects With   |  |          |   | 5                        |                           |
| 1.7         | Identification and Authentication (IA)                   | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control |
| IA-1        | Identification and Authentication Policy and Procedures  | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days.  | Functional     | Intersects With   | Periodic Review & Update of Security, Compliance & Resilience Program            | GOV-03   | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRIP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.  | 5                        |                           |
| IA-1        | Identification and Authentication Policy and Procedures  | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days.  | Functional     | Subset Of         | Identity & Access Management (IAM)   | IAC-01   | Mechanisms exist to facilitate the implementation of identification and access management controls.   | 10                       |                           |
| IA-1        | Identification and Authentication Policy and Procedures  | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days.  | Functional     | Intersects With   | Publishing Security, Compliance & Resilience Documentation                       | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.  | 5                        |                           |
| IA-1.a      | Identification and Authentication Policy and Procedures  | A formal, documented identification and authentication policy that addresses system scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and   | Functional     | Subset Of         | Publishing Security, Compliance & Resilience Documentation                       | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.  | 10                       |                           |
| IA-1.b      | Identification and Authentication Policy and Procedures  | Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.  | Functional     | Subset Of         | Standardized Operating Procedures (SOP)  | OPS-01.1 | Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.   | 10                       |                           |
| IA-2        | Identification and Authentication (Organizational Users) | The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).   | Functional     | Subset Of         | 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-2-1.1    | Identification and Authentication (Organizational Users) | Require the use of system and/or network authenticators and unique user identifiers.   | Functional     | Subset Of         | 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-2-1.2    | Identification and Authentication (Organizational Users) | Help desk support requires user identification for any transaction that has information security implications.   | Functional     | Subset Of         | 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-2-1.3    | Identification and Authentication (Organizational Users) | Follow CMS guidance provided in the Electronic Authentication Guidelines for ACA Administering Entity Systems, which can be found at: <a href="https://calt.cms.gov/projects/cms_ica_program_security_privacy/">https://calt.cms.gov/projects/cms_ica_program_security_privacy/</a> .  | Functional     | Subset Of         | 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-2(1)     | Network Access to Privileged Accounts                    | The information system implements multifactor authentication for network 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/regulatory data.                                    | 5                        |                           |
| IA-2(1)     | Network Access to Privileged Accounts                    | The information system implements multifactor authentication for network 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-2(1)     | Network Access to Privileged Accounts                    | The information system implements multifactor authentication for network 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-approved. | 5                        |                           |
| IA-2(1)     | Network Access to Privileged Accounts                    | The information system implements multifactor authentication for network 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-2(1)     | Network Access to Privileged Accounts                    | The information system implements multifactor authentication for network 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-2(1)     | Network Access to Privileged Accounts                    | The information system implements multifactor authentication for network 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-2(1)     | Network Access to Privileged Accounts                    | The information system implements multifactor authentication for network 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-2(2)     | Network Access to Non-Privileged Accounts                | The information system implements multifactor authentication for network 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-approved. | 5                        |                           |
| IA-2(2)     | Network Access to Non-Privileged Accounts                | The information system implements multifactor authentication for network 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-2(2)     | Network Access to Non-Privileged Accounts                | The information system implements multifactor authentication for network 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-2(2)     | Network Access to Non-Privileged Accounts                | The information system implements multifactor authentication for network 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-2(2)     | Network Access to Non-Privileged Accounts                | The information system implements multifactor authentication for network 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                        |                           |

| FDE #       | FDE Name   | Focal Document Element (FDE) Description   | STRM Rationale | STRM Relationship | SCF Control  | SCF #    | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes                     |
|-------------|--|--|----------------|-------------------|--|----------|--|--------------------------|---------------------------|
| IA-2(2)     | Network Access to Non-Privileged Accounts                    | The information system implements multifactor authentication for network access to non-privileged accounts.  | Functional     | Intersects With   | Multi-Factor Authentication (MFA)                            | IA-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-2(2)     | Network Access to Non-Privileged Accounts                    | The information system implements multifactor authentication for network access to non-privileged accounts.  | Functional     | Intersects With   | Local Access to Privileged Accounts                          | IA-06.3  | Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.  | 5                        |                           |
| IA-2(3)     | Local Access to Privileged Accounts                          | The information system implements multifactor authentication for local access to privileged accounts.  | Functional     | Intersects With   | Local Access to Privileged Accounts                          | IA-06.3  | Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.  | 5                        |                           |
| IA-2(8)     | Network Access to Privileged Accounts - Replay Resistant     | The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.  | Functional     | Subset Of         | Replay-Resistant Authentication                              | IA-02.2  | Automated mechanisms exist to employ replay-resistant authentication.  | 10                       |                           |
| IA-2(11)    | Remote Access - Separate Device                              | The information system implements multifactor authentication for remote access to privileged and non-privileged accounts, assuring that one of the factors is provided by a device separate from the system gaining access.  | Functional     | Intersects With   | Multi-Factor Authentication (MFA)                            | IA-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-2(11)-5  | Remote Access - Separate Device                              | Reference CMS guidance provided in the Electronic Authentication Guidelines for ACA Administering Entity Systems, which can be found at: <a href="https://calt.cms.gov/projects/cms_aca_program_privacy/">https://calt.cms.gov/projects/cms_aca_program_privacy/</a> .   | Functional     | Subset Of         | Secure Baseline Configurations                               | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |                           |
| IA-3        | Device Identification and Authentication                     | The information system uniquely identifies and authenticates defined types of devices (defined in the applicable security plan) that require authentication mechanisms before establishing a connection that, at a minimum, use shared information (i.e., Media Access Control (MAC) or Internet Protocol (IP) address) and access control lists to control remote network access. | Functional     | Subset Of         | Identification & Authentication for Devices                  | IA-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.  | 10                       |                           |
| IA-3-5.1    | Device Identification and Authentication                     | The organization defines a list of specific devices and/or types of devices approved and accepted for identification and authentication management.  | Functional     | Subset Of         | Identification & Authentication for Devices                  | IA-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.  | 10                       |                           |
| IA-4        | Identifier Management  | The organization manages information system identifiers by:  | Functional     | Intersects With   | Authenticate, Authorize and Audit (AAA)                      | IA-01.2  | Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).   | 5                        |                           |
| IA-4        | Identifier Management  | The organization manages information system identifiers by:  | Functional     | Subset Of         | Identifier Management (User Names)                           | IA-09    | Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).  | 10                       |                           |
| IA-4.a      | Identifier Management  | Receiving authorization from defined personnel or roles (defined in the applicable security plan) to assign an individual, group, role, or device identifier;  | Functional     | Subset Of         | Identifier Management (User Names)                           | IA-09    | Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).  | 10                       |                           |
| IA-4.b      | Identifier Management  | Selecting an identifier that identifies an individual, group, role, or device;   | Functional     | Subset Of         | Identifier Management (User Names)                           | IA-09    | Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).  | 10                       |                           |
| IA-4.c      | Identifier Management  | Assigning the identifier to the intended individual, group, role, or device;   | Functional     | Subset Of         | Identifier Management (User Names)                           | IA-09    | Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).  | 10                       |                           |
| IA-4.d      | Identifier Management  | Preventing reuse of identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of at least two (2) years has expired; and   | Functional     | Subset Of         | Identifier Management (User Names)                           | IA-09    | Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).  | 10                       |                           |
| IA-4.e      | Identifier Management  | Disabling the identifier after sixty (60) days or less of inactivity and deleting disabled accounts during the annual re-certification process.  | Functional     | Subset Of         | Identifier Management (User Names)                           | IA-09    | Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).  | 10                       |                           |
| IA-4-5.1    | Identifier Management  | The organization prevents reuse of user or device identifiers for at least two (2) years and disables the user identifier after sixty (60) days of inactivity.   | Functional     | Subset Of         | Identifier Management (User Names)                           | IA-09    | Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).  | 10                       |                           |
| IA-4-5.2    | Identifier Management  | The organization defines time period of inactivity for device identifiers.   | Functional     | Subset Of         | Identifier Management (User Names)                           | IA-09    | Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).  | 10                       |                           |
| IA-5        | Authenticator Management                                     | The organization manages information system authenticators by:   | Functional     | Intersects With   | Authenticator Management (User Names)                        | IA-10    | Mechanisms exist to (1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.  | 5                        |                           |
| IA-5        | Authenticator Management                                     | The organization manages information system authenticators by:   | Functional     | Intersects With   | Default Authenticators                                       | IA-10.8  | Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.  | 5                        |                           |
| IA-5(1)     | Password-Based Authentication                                | For password-based authentication, the information systems follow the direction in the applicable configuration baselines per CM-6, or as follows, whichever is more stringent:  | Functional     | Intersects With   | Automated Support For Password Strength                      | IA-10.4  | Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.   | 5                        |                           |
| IA-5(1)     | Password-Based Authentication                                | For password-based authentication, the information systems follow the direction in the applicable configuration baselines per CM-6, or as follows, whichever is more stringent:  | Functional     | Subset Of         | Password-Based Authentication                                | IA-10.1  | Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.  | 10                       |                           |
| IA-5(1)     | Password-Based Authentication                                | For password-based authentication, the information systems follow the direction in the applicable configuration baselines per CM-6, or as follows, whichever is more stringent:  | Functional     | Intersects With   | Authenticator Management                                     | IA-10    | Mechanisms exist to (1) Securely manage authenticators for users and devices; and(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.  | 5                        |                           |
| IA-5(1).a   | Password-Based Authentication                                | Allows the use of a temporary password for system logons with an immediate change to a permanent password.   | Functional     | Subset Of         | Password-Based Authentication                                | IA-10.1  | Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.  | 10                       |                           |
| IA-5(1).b   | Password-Based Authentication                                | Password Complexity: User/Privileged Accounts: Eight (8) characters; at least one numeric and at least one special character; a mixture of at least one uppercase and at least one lowercase letter;   | Functional     | Subset Of         | Password-Based Authentication                                | IA-10.1  | Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.  | 10                       |                           |
| IA-5(1).c   | Password-Based Authentication                                | Prohibits the use of dictionary names or words;  | Functional     | Subset Of         | Password-Based Authentication                                | IA-10.1  | Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.  | 10                       |                           |
| IA-5(1).d   | Password-Based Authentication                                | Enforces at least the following minimum password requirements for Users / Privileged Users / Processes (acting on behalf of a User):   | Functional     | Subset Of         | Password-Based Authentication                                | IA-10.1  | Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.  | 10                       |                           |
| IA-5(1).d.1 | Password-Based Authentication                                | MinimumPasswordAge = 1/1 ;   | Functional     | Subset Of         | Password-Based Authentication                                | IA-10.1  | Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.  | 10                       |                           |
| IA-5(1).d.2 | Password-Based Authentication                                | MaximumPasswordAge = 60/60/180   | Functional     | Subset Of         | Password-Based Authentication                                | IA-10.1  | Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.  | 10                       |                           |
| IA-5(1).d.3 | Password-Based Authentication                                | MinimumPasswordlength = 8/8/15   | Functional     | Subset Of         | Password-Based Authentication                                | IA-10.1  | Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.  | 10                       |                           |
| IA-5(1).e   | Password-Based Authentication                                | Enforces at least four (4) changed characters or as determined by the information system (where possible) when new passwords are created;  | Functional     | Subset Of         | Password-Based Authentication                                | IA-10.1  | Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.  | 10                       |                           |
| IA-5(1).f   | Password-Based Authentication                                | Stores and transmits only cryptographically protected passwords;   | Functional     | Subset Of         | Password-Based Authentication                                | IA-10.1  | Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.  | 10                       |                           |
| IA-5(1).g   | Password-Based Authentication                                | Prohibit password reuse for 24 generations; and  | Functional     | Subset Of         | Password-Based Authentication                                | IA-10.1  | Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.  | 10                       |                           |
| IA-5(1).h   | Password-Based Authentication                                | Password-protect system initialization (boot) settings   | Functional     | Subset Of         | Password-Based Authentication                                | IA-10.1  | Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.  | 10                       |                           |
| IA-5(2)     | PKI-Based Authentication                                     | For PKI-based authentication, the information system:  | Functional     | Subset Of         | PKI-Based Authentication                                     | IA-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-5(2).a   | PKI-Based Authentication                                     | Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;   | Functional     | Subset Of         | PKI-Based Authentication                                     | IA-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-5(2).b   | PKI-Based Authentication                                     | Enforces authorized access to the corresponding private key;   | Functional     | Subset Of         | PKI-Based Authentication                                     | IA-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-5(2).c   | PKI-Based Authentication                                     | Maps the authenticated identity to the account of the individual or group; and   | Functional     | Subset Of         | PKI-Based Authentication                                     | IA-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-5(2).d   | PKI-Based Authentication                                     | Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.  | Functional     | Subset Of         | PKI-Based Authentication                                     | IA-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-5(3)     | In-Person or Trusted Third Party Registration                | The organization requires that the registration process to receive hardware administrative tokens and credentials used for two (2)-factor authentication be conducted in person before a designated registration authority with authorization by defined personnel or roles (defined in the applicable security plan).   | Functional     | Subset Of         | In-Person or Trusted Third-Party Registration                | IA-10.3  | Mechanisms exist to conduct in-person or trusted third-party identify verification before user accounts for third-parties are created.   | 10                       |                           |
| IA-5(7)     | No Embedded Unencrypted Static Authenticators                | The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.   | Functional     | Subset Of         | No Embedded Unencrypted Static Authenticators                | IA-10.6  | Mechanisms exist to ensure that unencrypted, static authenticators are not embedded in applications, scripts or stored on function keys.   | 10                       |                           |
| IA-5(11)    | Hardware Token-Based Authentication                          | The information system, for hardware token-based authentication, employs mechanisms that satisfy minimum token requirements.   | Functional     | Subset Of         | Hardware Token-Based Authentication                          | IA-10.7  | Automated mechanisms exist to ensure organization-defined token quality requirements are satisfied for hardware token-based authentication.  | 10                       |                           |
| IA-6        | Authenticator Feedback                                       | The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.  | Functional     | Subset Of         | Authenticator Feedback                                       | IA-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-7        | Cryptographic Module Authentication                          | The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.   | Functional     | Intersects With   | Cryptographic Module Authentication                          | IA-12    | Mechanisms exist to ensure cryptographic modules adhere to applicable statutory, regulatory and contractual requirements for security strength.  | 5                        |                           |
| IA-7        | Cryptographic Module Authentication                          | The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.   | Functional     | Intersects With   | Automated Authentication Through Cryptographic Modules       | CRY-02   | Automated mechanisms exist to enable systems to authenticate to a cryptographic module.  | 5                        |                           |
| IA-8        | Identification and Authentication (Non-Organizational Users) | The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).   | Functional     | Subset Of         | Identification & Authentication for Non-Organizational Users | IA-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-8-5      | Identification and Authentication (Non-Organizational Users) | Follow CMS guidance provided in the Electronic Authentication Guidelines for ACA Administering Entity Systems, which can be found at: <a href="https://calt.cms.gov/projects/cms_aca_program_privacy/">https://calt.cms.gov/projects/cms_aca_program_privacy/</a> .  | Functional     | Subset Of         | Identification & Authentication for Non-Organizational Users | IA-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                       |                           |
| 1.8         | Incident Response (IR)                                       | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A  | 0                        | No applicable SCF control |
| IR-1        | Incident Response Policy and Procedures                      | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days;  | Functional     | Intersects With   | Publishing Security, Compliance & Resilience Documentation   | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.   | 5                        |                           |
| IR-1        | Incident Response Policy and Procedures                      | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days;  | Functional     | Subset Of         | Incident Response Operations                                 | IRO-01   | Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.   | 10                       |                           |
| IR-1        | Incident Response Policy and Procedures                      | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days;  | Functional     | Intersects With   | IRP Update   | IRO-04.2 | Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.  | 5                        |                           |
| IR-1        | Incident Response Policy and Procedures                      | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days;  | 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                        |                           |

| FDE #    | FDE Name   | Focal Document Element (FDE) Description   | STRM Rationale | STRM Relationship | SCF Control   | SCF #    | Secure Controls Framework (SCF) Control Description   | Strength of Relationship | Notes  |
|----------|--|--|----------------|-------------------|---|----------|---|--------------------------|--|
| IR-1     | Incident Response Policy and Procedures                    | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:  | Functional     | Intersects With   | Periodic Review & Update of Security, Compliance & Resilience Program | GOV-03   | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. | 5                        |  |
| IR-1.a   | Incident Response Policy and Procedures                    | An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and   | Functional     | Subset Of         | Publishing Security, Compliance & Resilience Documentation            | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.  | 10                       |  |
| IR-1.b   | Incident Response Policy and Procedures                    | Procedures to facilitate the implementation of the incident response policy and associated incident response controls.   | Functional     | Subset Of         | Standardized Operating Procedures (SOP)                               | OPS-01.1 | Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.   | 10                       |  |
| IR-2     | Incident Response Training                                 | N/A  | Functional     | Subset Of         | Incident Response Training  | IRO-05   | Mechanisms exist to train personnel in their incident response roles and responsibilities.  | 10                       |  |
| IR-2-1   | Incident Response Training                                 | The organization provides incident response training consistent with assigned roles and responsibilities to information system users.  | Functional     | Subset Of         | Incident Response Training  | IRO-05   | Mechanisms exist to train personnel in their incident response roles and responsibilities.  | 10                       | Overlapping subpoint letters, first of series  |
| IR-2-1a  | Incident Response Training                                 | Within ninety (90) days of assuming an incident response role or responsibility;   | Functional     | Subset Of         | Incident Response Training  | IRO-05   | Mechanisms exist to train personnel in their incident response roles and responsibilities.  | 10                       | Overlapping subpoint letters, first of series  |
| IR-2-1b  | Incident Response Training                                 | When required by information system changes; and   | Functional     | Subset Of         | Incident Response Training  | IRO-05   | Mechanisms exist to train personnel in their incident response roles and responsibilities.  | 10                       | Overlapping subpoint letters, first of series  |
| IR-2-1c  | Incident Response Training                                 | Within every three hundred sixty-five (365) days thereafter.   | Functional     | Subset Of         | Incident Response Training  | IRO-05   | Mechanisms exist to train personnel in their incident response roles and responsibilities.  | 10                       | Overlapping subpoint letters, first of series  |
| IR-2-2   | Incident Response Training                                 | The organization:  | Functional     | Subset Of         | Incident Response Training  | IRO-05   | Mechanisms exist to train personnel in their incident response roles and responsibilities.  | 10                       |  |
| IR-2-2a  | Incident Response Training                                 | Identifies employees with significant information security responsibilities and provides role-specific training in accordance with NIST standards and guidance;  | Functional     | Subset Of         | Incident Response Training  | IRO-05   | Mechanisms exist to train personnel in their incident response roles and responsibilities.  | 10                       | Overlapping subpoint letters, second of series |
| IR-2-2b  | Incident Response Training                                 | Includes user training in the identification and reporting of suspicious activities, both from external and internal sources.  | Functional     | Subset Of         | Incident Response Training  | IRO-05   | Mechanisms exist to train personnel in their incident response roles and responsibilities.  | 10                       | Overlapping subpoint letters, second of series |
| IR-2-2c  | Incident Response Training                                 | Exposes all information systems users (i.e., employees, contractors, students, guest researchers, visitors, and others who may need access to information systems and applications) to security awareness materials addressing IR response associated with the roles. For example, regular users may only need to know whom to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. | Functional     | Subset Of         | Incident Response Training  | IRO-05   | Mechanisms exist to train personnel in their incident response roles and responsibilities.  | 10                       | Overlapping subpoint letters, second of series |
| IR-2-2d  | Incident Response Training                                 | Provides information systems security refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees uses or processes and their role.   | Functional     | Subset Of         | Incident Response Training  | IRO-05   | Mechanisms exist to train personnel in their incident response roles and responsibilities.  | 10                       | Overlapping subpoint letters, second of series |
| IR-3     | Incident Response Testing                                  | The organization:  | Functional     | Subset Of         | Incident Response Testing   | IRO-06   | Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.  | 10                       |  |
| IR-3.a   | Incident Response Testing                                  | Tests the incident response capability for the information system, reviews and analyzes the results, performs simulations, and documents the test results to determine the incident response effectiveness within every three hundred sixty-five (365) days using NIST SP 800-61;  | Functional     | Subset Of         | Incident Response Testing   | IRO-06   | Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.  | 10                       |  |
| IR-3.b   | Incident Response Testing                                  | Must produce an after-action report to improve existing processes, procedures, and policies;   | Functional     | Subset Of         | Incident Response Testing   | IRO-06   | Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.  | 10                       |  |
| IR-3.c   | Incident Response Testing                                  | Need not conduct a formal test if the organization actively exercises its response capability using real incidents.  | Functional     | Subset Of         | Incident Response Testing   | IRO-06   | Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.  | 10                       |  |
| IR-3(2)  | Coordination with Related Plans                            | The organization coordinates incident response testing with organizational elements responsible for related plans.   | Functional     | Subset Of         | Incident Response Testing   | IRO-06   | Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.  | 10                       |  |
| IR-4     | Incident Handling  | The organization:  | Functional     | Subset Of         | 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-4.a   | Incident Handling  | Implements an incident handling capability using the current Administering Entity (AE) organization Procedure for Incident Handling.   | Functional     | Subset Of         | 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-4.b   | Incident Handling  | Coordinates incident handling activities with contingency planning activities;   | Functional     | Subset Of         | 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-4.c   | Incident Handling  | Documents relevant information related to an security incident according to the current AE organization and ACA-required procedures;   | Functional     | Subset Of         | 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-4.d   | Incident Handling  | Preserves evidence through technical means, including secured storage of evidence media and "write" protection of evidence media; uses sound forensics processes and utilities that support legal requirements; And determines and follows chain of custody for forensic evidence;   | Functional     | Subset Of         | 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-4.e   | Incident Handling  | Identifies vulnerability exploited during a security incident;   | Functional     | Subset Of         | 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-4.f   | Incident Handling  | Implements security safeguards to reduce risk and vulnerability exploit exposure;  | Functional     | Subset Of         | 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-4.g   | Incident Handling  | Ensures that the individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information processed, stored, and transmitted by the information system; and  | Functional     | Subset Of         | 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-4.h   | Incident Handling  | Incorporates lessons learned from ongoing incident handling activities into AE incident response procedures, training, and testing, and implements the resulting changes accordingly.  | Functional     | Subset Of         | 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-4(5)  | Incident Handling  | Follow CMS guidance for Incident Handling, which can be found at: <a href="https://calt.cms.gov/objects/cms_aca_program_security_privacy/">https://calt.cms.gov/objects/cms_aca_program_security_privacy/</a> .  | Functional     | Subset Of         | 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-4(1)  | Automated Incident Handling Processes                      | The organization employs automated mechanisms to support the incident handling process.  | Functional     | Subset Of         | Automated Incident Handling Processes                                 | IRO-02.1 | Automated mechanisms exist to support the incident handling process.  | 10                       |  |
| IR-5     | Incident Monitoring  | The organization tracks and documents information system security incidents.   | Functional     | Subset Of         | 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-6     | Incident Reporting   | The organization:  | Functional     | Subset Of         | Incident Stakeholder Reporting  | IRO-10   | Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.  | 10                       |  |
| IR-6     | Incident Reporting   | The organization:  | Functional     | Intersects With   | Regulatory & Law Enforcement Contacts                                 | IRO-14   | Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.  | 5                        |  |
| IR-6     | Incident Reporting   | The organization:  | Functional     | Intersects With   | Contacts With Authorities   | GOV-06   | Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.   | 5                        |  |
| IR-6.a   | Incident Reporting   | Requires personnel to report suspected incidents to the organizational incident response capability within the timeframe established in the CMS guidance for Incident Handling and using the Administering Entity Security and Privacy Incident Report template, which can be found at: <a href="https://calt.cms.gov/objects/cms_aca_program_security_privacy/">https://calt.cms.gov/objects/cms_aca_program_security_privacy/</a> ; and  | Functional     | Subset Of         | Incident Stakeholder Reporting  | IRO-10   | Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.  | 10                       |  |
| IR-6.b   | Incident Reporting   | Reports security incident information to designated authorities.   | Functional     | Subset Of         | Incident Stakeholder Reporting  | IRO-10   | Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.  | 10                       |  |
| IR-6(1)  | Automated Reporting  | The organization employs automated mechanisms to assist in the reporting of security incidents.  | Functional     | Subset Of         | Automated Reporting   | IRO-10.1 | Automated mechanisms exist to assist in the reporting of cybersecurity and data protection incidents.   | 10                       |  |
| IR-7     | Incident Response Assistance                               | The organization provides an incident response support resource integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.   | Functional     | Subset Of         | 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-7(1)  | Automation Support for Availability of Information/Support | The organization employs automated mechanisms to increase the availability of incident response-related information and support.   | Functional     | Subset Of         | 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-8     | Incident Response Plan                                     | The organization:  | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.  | 10                       |  |
| IR-8.a   | Incident Response Plan                                     | Develops an incident response plan that:   | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.  | 10                       |  |
| IR-8.a.1 | Incident Response Plan                                     | Provides the organization with a roadmap for implementing its incident response plan;  | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.  | 10                       |  |
| IR-8.a.2 | Incident Response Plan                                     | Describes the structure and organization of the incident response capability;  | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.  | 10                       |  |
| IR-8.a.3 | Incident Response Plan                                     | Provides a high-level approach for how the incident response capability fits into the overall organization;  | Functional     | Subset Of         | 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                       |  |

| FDE #          | FDE Name                                 | Focal Document Element (FDE) Description  | STRM Rationale | STRM Relationship | SCF Control   | SCF #    | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes                     |
|----------------|--|---|----------------|-------------------|---|----------|--|--------------------------|---------------------------|
| IR-8.a.4       | Incident Response Plan                   | Meets the unique requirements of the organization, which relate to mission, size, structure, and functions.   | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.   | 10                       |                           |
| IR-8.a.5       | Incident Response Plan                   | Defines repeatable incidents.   | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.   | 10                       |                           |
| IR-8.a.6       | Incident Response Plan                   | Provides metrics for measuring the incident response capability within the organization.  | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.   | 10                       |                           |
| IR-8.a.7       | Incident Response Plan                   | Defines the resources and management support needed to effectively maintain and make available incident response capability.  | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.   | 10                       |                           |
| IR-8.a.8       | Incident Response Plan                   | Is reviewed and approved by the applicable Incident Response Team Leader.   | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.   | 10                       |                           |
| IR-8.a.9       | Incident Response Plan                   | Is distributed to identified incident response personnel and organizational units, which may include:   | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.   | 10                       |                           |
| IR-8.a.9(i)    | Incident Response Plan                   | Chief Information Security Officer;   | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.   | 10                       |                           |
| IR-8.a.9(ii)   | Incident Response Plan                   | Chief Information Officer;  | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.   | 10                       |                           |
| IR-8.a.9(iii)  | Incident Response Plan                   | Information System Security Officer;  | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.   | 10                       |                           |
| IR-8.a.9(iv)   | Incident Response Plan                   | Attorney General/Computer Crimes Unit;  | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.   | 10                       |                           |
| IR-8.a.9(v)    | Incident Response Plan                   | Personnel within the organization Incident Response Team;   | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.   | 10                       |                           |
| IR-8.a.9(vi)   | Incident Response Plan                   | Personnel within the Personally Identifiable Information (PII) Breach Response Team; and  | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.   | 10                       |                           |
| IR-8.a.9(vii)  | Incident Response Plan                   | Personnel within the organization Operations Centers;   | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.   | 10                       |                           |
| IR-8.a.9(viii) | Incident Response Plan                   | CMS   | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.   | 10                       |                           |
| IR-8.b         | Incident Response Plan                   | Reviews within every three hundred sixty-five (365) days;   | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.   | 10                       |                           |
| IR-8.c         | Incident Response Plan                   | Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;  | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.   | 10                       |                           |
| IR-8.d         | Incident Response Plan                   | Communicates incident response plan changes to the organizational elements listed in (ii) above; and  | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.   | 10                       |                           |
| IR-8.e         | Incident Response Plan                   | The incident response plan from unauthorized disclosure and modification.   | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.   | 10                       |                           |
| IR-8-IS.1      | Incident Response Plan                   | The organization defines a list of incident response personnel (identified by name and/or by role) and organizational elements for distribution of the response plan. The incident response list includes designated CMS personnel.   | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.   | 10                       |                           |
| IR-8-IS.2      | Incident Response Plan                   | The organization defines a list of incident response personnel (identified by name and/or by role) and organizational elements for communication of any changes. The incident response list includes designated CMS personnel.  | Functional     | Subset Of         | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.   | 10                       |                           |
| IR-8-IS.3      | Incident Response Plan                   | Follow CMS guidance for Incident Handling, which can be found at: <a href="https://calt.cms.gov/sf/projects/cms_eca_program_security_privacy/">https://calt.cms.gov/sf/projects/cms_eca_program_security_privacy/</a> .   | Functional     | Subset Of         | 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-9           | Information Spillage Response            | The organization responds to information spills by:   | Functional     | Subset Of         | Sensitive / Regulated Data Spill Response                             | IRO-12   | Mechanisms exist to respond to sensitive/regulated data spills.  | 10                       |                           |
| IR-9           | Information Spillage Response            | The organization responds to information spills by:   | Functional     | Intersects With   | Sensitive / Regulated Data Spill Response                             | IRO-12.1 | Mechanisms exist to formally assign personnel or roles with responsibility for responding to sensitive/regulated data spills.  | 5                        |                           |
| IR-9.a         | Information Spillage Response            | Requiring personnel to report suspected incidents to the organizational incident response capability within the timeframe established in the current Administering Entity (AE) organization Incident Handling Procedure and ACA incident handling reporting process available at: <a href="https://calt.cms.gov/sf/projects/cms_eca_program_security_privacy/">https://calt.cms.gov/sf/projects/cms_eca_program_security_privacy/</a> . | Functional     | Subset Of         | Sensitive / Regulated Data Spill Response                             | IRO-12   | Mechanisms exist to respond to sensitive/regulated data spills.  | 10                       |                           |
| IR-9.b         | Information Spillage Response            | Identifying the specific information involved in the improper or potentially improper information disclosure.   | Functional     | Subset Of         | Sensitive / Regulated Data Spill Response                             | IRO-12   | Mechanisms exist to respond to sensitive/regulated data spills.  | 10                       |                           |
| IR-9.c         | Information Spillage Response            | Alerting authorized incident response personnel of the information spill using a method of communication not associated with the spill.   | Functional     | Subset Of         | Sensitive / Regulated Data Spill Response                             | IRO-12   | Mechanisms exist to respond to sensitive/regulated data spills.  | 10                       |                           |
| IR-9.d         | Information Spillage Response            | Identifying other information systems or system components on which the information may have been subsequently improperly or potentially improperly shared with or disclosed to; and  | Functional     | Subset Of         | Sensitive / Regulated Data Spill Response                             | IRO-12   | Mechanisms exist to respond to sensitive/regulated data spills.  | 10                       |                           |
| IR-9.e         | Information Spillage Response            | Removing and destroying the information from the contaminated information system, component or individual not authorized to handle the information.   | Functional     | Subset Of         | Sensitive / Regulated Data Spill Response                             | IRO-12   | Mechanisms exist to respond to sensitive/regulated data spills.  | 10                       |                           |
| 1.9            | Maintenance (MA)                         | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control |
| MA-1           | System Maintenance Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days.   | Functional     | Subset Of         | Maintenance Operations  | MNT-01   | Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.   | 10                       |                           |
| MA-1           | System Maintenance Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days.   | Functional     | Intersects With   | Remote Maintenance Notifications                                      | MNT-05.2 | Mechanisms exist to require maintenance personnel to notify affected stakeholders when remote, non-local maintenance is planned (e.g., date/time).   | 5                        |                           |
| MA-1           | System Maintenance Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days.   | Functional     | Intersects With   | Auditing Remote Maintenance   | MNT-05.1 | Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.  | 5                        |                           |
| MA-1           | System Maintenance Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days.   | Functional     | Intersects With   | Periodic Review & Update of Security, Compliance & Resilience Program | GOV-03   | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRIP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. | 5                        |                           |
| MA-1           | System Maintenance Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days.   | Functional     | Intersects With   | Publishing Security, Compliance & Resilience Documentation            | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.   | 5                        |                           |
| MA-1.a         | System Maintenance Policy and Procedures | A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  | Functional     | Subset Of         | Publishing Security, Compliance & Resilience Documentation            | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.   | 10                       |                           |
| MA-1.b         | System Maintenance Policy and Procedures | Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls.  | Functional     | Subset Of         | Standardized Operating Procedures (SOP)                               | OPS-01.1 | Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.  | 10                       |                           |
| MA-2           | Controlled Maintenance                   | The organization:   | Functional     | Subset Of         | Controlled Maintenance  | MNT-02   | Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).   | 10                       |                           |
| MA-2.a         | Controlled Maintenance                   | Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;  | Functional     | Subset Of         | Controlled Maintenance  | MNT-02   | Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).   | 10                       |                           |
| MA-2.b         | Controlled Maintenance                   | Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;   | Functional     | Subset Of         | Controlled Maintenance  | MNT-02   | Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).   | 10                       |                           |
| MA-2.c         | Controlled Maintenance                   | Requires that the applicable business owner (or an official designated in the applicable security plan) explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;   | Functional     | Subset Of         | Controlled Maintenance  | MNT-02   | Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).   | 10                       |                           |
| MA-2.d         | Controlled Maintenance                   | Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;  | Functional     | Subset Of         | Controlled Maintenance  | MNT-02   | Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).   | 10                       |                           |
| MA-2.e         | Controlled Maintenance                   | Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and   | Functional     | Subset Of         | Controlled Maintenance  | MNT-02   | Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).   | 10                       |                           |
| MA-2.f         | Controlled Maintenance                   | Includes defined maintenance-related information (defined in the applicable security plan) in organizational maintenance records.   | Functional     | Subset Of         | Controlled Maintenance  | MNT-02   | Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).   | 10                       |                           |
| MA-2-IS.1      | Controlled Maintenance                   | In facilities where Personally Identifiable Information (PII) is stored or accessed, document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks).   | Functional     | Subset Of         | 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-3           | Maintenance Tools                        | The organization approves, controls, and monitors information system maintenance tools.   | Functional     | Intersects With   | Maintenance Tools   | MNT-04   | Mechanisms exist to control and monitor the use of system maintenance tools.   | 5                        |                           |
| MA-3(1)        | Inspect Tools                            | The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.  | Functional     | Subset Of         | Inspect Tools   | MNT-04.1 | Mechanisms exist to inspect maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.   | 10                       |                           |
| MA-3(2)        | Inspect Media                            | The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.   | Functional     | Subset Of         | 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-3(3)        | Prevent Unauthorized Removal             | The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:   | Functional     | Subset Of         | Prevent Unauthorized Removal  | MNT-04.3 | Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational information.   | 10                       |                           |
| MA-3(3).a      | Prevent Unauthorized Removal             | Verifying that there is no organizational information contained on the equipment;   | Functional     | Subset Of         | Prevent Unauthorized Removal  | MNT-04.3 | Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational information.   | 10                       |                           |
| MA-3(3).b      | Prevent Unauthorized Removal             | Sanitizing or destroying the equipment;   | Functional     | Subset Of         | Prevent Unauthorized Removal  | MNT-04.3 | Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational information.   | 10                       |                           |
| MA-3(3).c      | Prevent Unauthorized Removal             | Retaining the equipment within the facility; or   | Functional     | Subset Of         | Prevent Unauthorized Removal  | MNT-04.3 | Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational information.   | 10                       |                           |
| MA-3(3).d      | Prevent Unauthorized Removal             | Obtaining an exemption, in writing, from the CIO or his/her designated representative explicitly authorizing removal of the equipment from the facility.  | Functional     | Subset Of         | Prevent Unauthorized Removal  | MNT-04.3 | Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational information.   | 10                       |                           |
| MA-4           | Nonlocal Maintenance                     | The organization monitors and controls nonlocal maintenance and diagnostic activities; and prohibits nonlocal system maintenance unless explicitly authorized, in writing, by the CIO or his/her designated representative. If nonlocal maintenance and diagnostic activities are authorized, the organization:   | Functional     | Subset Of         | Remote Maintenance  | MNT-05   | Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.  | 10                       |                           |
| MA-4           | Nonlocal Maintenance                     | The organization monitors and controls nonlocal maintenance and diagnostic activities; and prohibits nonlocal system maintenance unless explicitly authorized, in writing, by the CIO or his/her designated representative. If nonlocal maintenance and diagnostic activities are authorized, the organization:   | 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-4           | Nonlocal Maintenance                     | The organization monitors and controls nonlocal maintenance and diagnostic activities; and prohibits nonlocal system maintenance unless explicitly authorized, in writing, by the CIO or his/her designated representative. If nonlocal maintenance and diagnostic activities are authorized, the organization:   | 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-4.a         | Nonlocal Maintenance                     | Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;   | Functional     | Subset Of         | Remote Maintenance  | MNT-05   | Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.  | 10                       |                           |
| MA-4.b         | Nonlocal Maintenance                     | Employs multi-factor authentication in the establishment of nonlocal maintenance and diagnostic sessions;   | Functional     | Subset Of         | Remote Maintenance  | MNT-05   | Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.  | 10                       |                           |
| MA-4.c         | Nonlocal Maintenance                     | Maintains records for nonlocal maintenance and diagnostic activities; and   | Functional     | Subset Of         | Remote Maintenance  | MNT-05   | Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.  | 10                       |                           |
| MA-4.d         | Nonlocal Maintenance                     | Terminates all sessions and network connections when nonlocal maintenance is completed.   | Functional     | Subset Of         | Remote Maintenance  | MNT-05   | Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.  | 10                       |                           |
| MA-4(1)        | Auditing and Review                      | The organization:   | Functional     | Subset Of         | 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.  | 10                       |                           |
| MA-4(1).a      | Auditing and Review                      | Audits nonlocal maintenance and diagnostic sessions using available audit events; and   | Functional     | Subset Of         | 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.  | 10                       |                           |
| MA-4(1).b      | Auditing and Review                      | Reviews the records of the maintenance and diagnostic sessions.   | Functional     | Subset Of         | 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.  | 10                       |                           |

| FDE #     | FDE Name                               | Focal Document Element (FDE) Description   | STRM Rationale | STRM Relationship | SCF Control   | SCF #    | Secure Controls Framework (SCF) Control Description   | Strength of Relationship | Notes                     |
|-----------|--|--|----------------|-------------------|---|----------|---|--------------------------|---------------------------|
| MA-4(2)   | Document Nonlocal Maintenance          | The organization documents in the information system's security plan the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.   | Functional     | Subset Of         | Remote Maintenance  | MNT-05   | Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.   | 10                       |                           |
| MA-4(3)   | Comparable Security/Sanitization       | The organization:<br>Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system serviced; or  | Functional     | Subset Of         | 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-4(3).a | Comparable Security/Sanitization       | Removes the component to be serviced from the information system prior to nonlocal maintenance or diagnostic services; sanitizes the component (with regard to organizational information) before removal from organizational files; and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.   | Functional     | Subset Of         | 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-5      | Maintenance Personnel                  | The organization:<br>Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;<br>Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and<br>Designates 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     | Subset Of         | Authorized Maintenance Personnel                                      | MNT-06   | Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.   | 10                       |                           |
| MA-5.a    | Maintenance Personnel                  | Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;   | Functional     | Subset Of         | Authorized Maintenance Personnel                                      | MNT-06   | Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.   | 10                       |                           |
| MA-5.b    | Maintenance Personnel                  | Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and  | Functional     | Subset Of         | Authorized Maintenance Personnel                                      | MNT-06   | Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.   | 10                       |                           |
| MA-5.c    | Maintenance Personnel                  | Designates 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     | Subset Of         | Authorized Maintenance Personnel                                      | MNT-06   | Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.   | 10                       |                           |
| MA-6      | Timely Maintenance                     | The organization obtains maintenance support and/or spare parts for defined key information system components (defined in the applicable security plan) within the applicable Recovery Time Objective (RTO) specified in the contingency plan.   | Functional     | Subset Of         | Timely Maintenance  | MNT-03   | Mechanisms exist to obtain maintenance support and/or spare parts for Technology Assets, Applications and/or Services (TAAS) within a defined Recovery Time Objective (RTO).  | 10                       |                           |
| 1.10      | Media Protection (MP)                  | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A   | 0                        | No applicable SCF control |
| MP-1      | Media Protection Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as applicable), within every three hundred sixty-five (365) days:   | Functional     | Intersects With   | Periodic Review & Update of Security, Compliance & Resilience Program | GOV-03   | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.   | 5                        |                           |
| MP-1      | Media Protection Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as applicable), within every three hundred sixty-five (365) days:   | Functional     | Subset Of         | Data Protection   | DCH-01   | Mechanisms exist to facilitate the implementation of data protection controls.  | 10                       |                           |
| MP-1      | Media Protection Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as applicable), within every three hundred sixty-five (365) days:   | Functional     | Intersects With   | Publishing Security, Compliance & Resilience Documentation            | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.  | 5                        |                           |
| MP-1.a    | Media Protection Policy and Procedures | A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and   | Functional     | Subset Of         | Publishing Security, Compliance & Resilience Documentation            | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.  | 10                       |                           |
| MP-1.b    | Media Protection Policy and Procedures | Procedures to facilitate the implementation of the media protection policy and associated media protection controls.   | Functional     | Subset Of         | Standardized Operating Procedures (SOP)                               | OPS-01.1 | Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.   | 10                       |                           |
| MP-1.5-1  | Media Protection Policy and Procedures | Semi-annual inventories of removable media containing Personally Identifiable Information (PII) are conducted. The organization accounts for any missing information by conducting PII documenting the search efforts and notifying the media initiator of the loss.   | Functional     | Subset Of         | Publishing Security, Compliance & Resilience Documentation            | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.  | 10                       |                           |
| MP-1.5-2  | Media Protection Policy and Procedures | Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, and digital video disks) and non-digital media (e.g., paper, microfilm).   | Functional     | Subset Of         | Standardized Operating Procedures (SOP)                               | OPS-01.1 | Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.   | 10                       |                           |
| MP-2      | Media Access                           | The organization restricts access to sensitive information, such as Personally Identifiable Information (PII), residing on digital and non-digital media to authorized individuals using automated mechanisms to control access to media storage areas.  | 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-2      | Media Access                           | The organization restricts access to sensitive information, such as Personally Identifiable Information (PII), residing on digital and non-digital media to authorized individuals using automated mechanisms to control access to media storage areas.  | Functional     | Intersects With   | Endpoint Device Management (EDM)                                      | END-01   | Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.   | 5                        |                           |
| MP-3      | Media Marking                          | The organization:<br>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.  | Functional     | Subset Of         | 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.  | 10                       |                           |
| MP-3      | Media Marking                          | The organization:<br>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.  | Functional     | Intersects With   | Automated Marking   | DCH-04.1 | 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-3.a    | Media Marking                          | Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and  | Functional     | Subset Of         | 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.  | 10                       |                           |
| MP-3.b    | Media Marking                          | Exempts specific types of media or hardware components, as specified, in writing, by the CIO or his/her designated representative, from marking as long as the media remain within a secure environment.   | Functional     | Subset Of         | 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.  | 10                       |                           |
| MP-4      | Media Storage                          | The organization:<br>Physically controls and securely stores all magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks within organization-defined controlled areas; encrypts digital media via a FIPS 140-2 validated encryption module; and for non-digital media, provides secure storage in locked cabinets or safes.  | Functional     | Subset Of         | Media Storage   | DCH-06   | Mechanisms exist to:<br>(1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and<br>(2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures. | 10                       |                           |
| MP-4.a    | Media Storage                          | Physically controls and securely stores all magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks within organization-defined controlled areas; encrypts digital media via a FIPS 140-2 validated encryption module; and for non-digital media, provides secure storage in locked cabinets or safes.   | Functional     | Subset Of         | Media Storage   | DCH-06   | Mechanisms exist to:<br>(1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and<br>(2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures. | 10                       |                           |
| MP-4.b    | Media Storage                          | Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.   | Functional     | Subset Of         | Media Storage   | DCH-06   | Mechanisms exist to:<br>(1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and<br>(2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures. | 10                       |                           |
| MP-4.5-1  | Media Storage                          | If Personally Identifiable Information (PII) is recorded on magnetic media with other data, it should be protected as if it were entirely PII.   | Functional     | Subset Of         | Media Storage   | DCH-06   | Mechanisms exist to:<br>(1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and<br>(2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures. | 10                       |                           |
| MP-5      | Media Transport                        | The organization:<br>Protects and controls digital and non-digital media containing sensitive information, such as Personally Identifiable Information (PII), during transport outside of controlled areas using cryptography and tamper-evident packaging, and (i) if hand-carried, using secureable container (e.g., locked briefcase) via authorized personnel, or (ii) if shipped, trackable with receipt by commercial carrier;   | Functional     | Subset Of         | Media Transportation  | DCH-07   | Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.   | 10                       |                           |
| MP-5.a    | Media Transport                        | Protects and controls digital and non-digital media containing sensitive information, such as Personally Identifiable Information (PII), during transport outside of controlled areas using cryptography and tamper-evident packaging, and (i) if hand-carried, using secureable container (e.g., locked briefcase) via authorized personnel, or (ii) if shipped, trackable with receipt by commercial carrier;  | Functional     | Subset Of         | Media Transportation  | DCH-07   | Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.   | 10                       |                           |
| MP-5.b    | Media Transport                        | Maintains accountability for information system media during transport outside of controlled areas;  | Functional     | Subset Of         | Media Transportation  | DCH-07   | Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.   | 10                       |                           |
| MP-5.c    | Media Transport                        | Documents activities associated with the transport of information system media; and  | Functional     | Subset Of         | Media Transportation  | DCH-07   | Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.   | 10                       |                           |
| MP-5.d    | Media Transport                        | Restricts the activities associated with the transport of information system media to authorized personnel.  | Functional     | Subset Of         | Media Transportation  | DCH-07   | Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.   | 10                       |                           |
| MP-5.5-1  | Media Transport                        | Protect and control PII media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel. PII must be in locked cabinets or sealed packing cartons while in transit.  | Functional     | Subset Of         | Media Transportation  | DCH-07   | Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.   | 10                       |                           |
| MP-5.5-2  | Media Transport                        | The organization protects and controls magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks during transport outside of controlled areas, and encrypts digital media via a FIPS 140-2 validated encryption module.  | Functional     | Subset Of         | Media Transportation  | DCH-07   | Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.   | 10                       |                           |
| MP-5.5-3  | Media Transport                        | The organization defines security measures to protect digital and non-digital media in transport.  | Functional     | Subset Of         | Media Transportation  | DCH-07   | Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.   | 10                       |                           |
| MP-5(4)   | Cryptographic Protection               | The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.   | Functional     | Subset Of         | 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.  | 10                       |                           |
| MP-6      | Media Sanitization                     | The organization:<br>Sanitizes both digital and non-digital information system media prior to disposal, release out of organizational control, or release for reuse using defined sanitization techniques and procedures (defined in the applicable security plan) in accordance with applicable federal and organizational standards and policies; and<br>Employs 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-6      | Media Sanitization                     | The organization:<br>Sanitizes both digital and non-digital information system media prior to disposal, release out of organizational control, or release for reuse using defined sanitization techniques and procedures (defined in the applicable security plan) in accordance with applicable federal and organizational standards and policies; and<br>Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.       | Functional     | Subset Of         | 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.   | 10                       |                           |
| MP-6      | Media Sanitization                     | The organization:<br>Sanitizes both digital and non-digital information system media prior to disposal, release out of organizational control, or release for reuse using defined sanitization techniques and procedures (defined in the applicable security plan) in accordance with applicable federal and organizational standards and policies; and<br>Employs 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-6.a    | Media Sanitization                     | Sanitizes both digital and non-digital information system media prior to disposal, release out of organizational control, or release for reuse using defined sanitization techniques and procedures (defined in the applicable security plan) in accordance with applicable federal and organizational standards and policies; and   | Functional     | Subset Of         | 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.   | 10                       |                           |
| MP-6.b    | Media Sanitization                     | Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.  | Functional     | Subset Of         | 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.   | 10                       |                           |
| MP-6.5-1  | Media Sanitization                     | Employ sanitization mechanisms consistent with guidance provided in NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization.   | Functional     | Subset Of         | 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.   | 10                       |                           |
| MP-6.5-2  | Media Sanitization                     | Finely shred hard-copy documents using approved equipment, techniques, and procedures, and with a minimum of cross-cut shredding.  | Functional     | Subset Of         | 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.   | 10                       |                           |

| FDE #           | FDE Name  | Focal Document Element (FDE) Description   | STRM Rationale | STRM Relationship | SCF Control   | SCF #    | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes                     |
|-----------------|---|--|----------------|-------------------|---|----------|--|--------------------------|---------------------------|
| MP-6-IS.3       | Media Sanitization  | Authorized employees of the receiving entity must be responsible for securing magnetic tape/cartridges before, during, and after processing, and they must ensure that the proper acknowledgment form is signed and returned. Inventory records must be maintained for purposes of control and accountability. Tapes containing Personally Identified Information, any hard-copy printout of a tape, or any file resulting from the processing of such a tape will be recorded in a log that identifies: | Functional     | Subset Of         | System Media Sanitization Documentation                               | DCH-09.1 | Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.  | 10                       |                           |
| MP-6-IS.3.a     | Media Sanitization  | Date received;   | Functional     | Subset Of         | System Media Sanitization Documentation                               | DCH-09.1 | Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.  | 10                       |                           |
| MP-6-IS.3.b     | Media Sanitization  | Reel/cartridge control number contents;  | Functional     | Subset Of         | System Media Sanitization Documentation                               | DCH-09.1 | Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.  | 10                       |                           |
| MP-6-IS.3.c     | Media Sanitization  | Number of records, if available;   | Functional     | Subset Of         | System Media Sanitization Documentation                               | DCH-09.1 | Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.  | 10                       |                           |
| MP-6-IS.3.d     | Media Sanitization  | Movement; and  | Functional     | Subset Of         | System Media Sanitization Documentation                               | DCH-09.1 | Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.  | 10                       |                           |
| MP-6-IS.3.e     | Media Sanitization  | If disposed of, the date and method of disposition.  | Functional     | Subset Of         | System Media Sanitization Documentation                               | DCH-09.1 | Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.  | 10                       |                           |
| MP-6-IS.4       | Media Sanitization  | Surplus equipment is stored securely while not in use, and disposed of or sanitized in accordance with NIST SP 800-88 Revision 3 when no longer required.  | Functional     | Subset Of         | 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.                                    | 10                       |                           |
| MP-6(I)         | Review/Approve/Track/Document/Verify                        | The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.   | Functional     | Subset Of         | System Media Sanitization Documentation                               | DCH-09.1 | Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.  | 10                       |                           |
| MP-6(I)-IS      | Review/Approve/Track/Document/Verify                        | The organization ensures Personally Identifiable Information is securely destroyed or disposed of in an appropriate and reasonable manner and in accordance with retention schedules.  | Functional     | Subset Of         | System Media Sanitization Documentation                               | DCH-09.1 | Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.  | 10                       |                           |
| MP-6(2)         | Equipment Testing - Enhancement                             | The organization tests sanitization equipment and procedures within every three hundred sixty-five (365) days to verify that the equipment is achieving the intended sanitization.   | Functional     | Subset Of         | Equipment Testing   | DCH-09.2 | Mechanisms exist to test sanitization equipment and procedures to verify that the intended result is achieved.   | 10                       |                           |
| MP-7            | Media Use   | The organization prohibits the use of personally owned media on organizational information systems or system components using defined security safeguards (defined in the applicable security plan).   | 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-7            | Media Use   | The organization prohibits the use of personally owned media on organizational information systems or system components using defined security safeguards (defined in the applicable security plan).   | 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-7            | Media Use   | The organization prohibits the use of personally owned media on organizational information systems or system components using defined security safeguards (defined in the applicable security plan).   | 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-7(1)         | Prohibit Use Without Owner                                  | The organization prohibits the use of portable storage devices in organizational information 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-CMS-1        | Media Related Records                                       | Inventory and disposition records for information system media shall be maintained to ensure control and accountability of sensitive information. The media-related records shall contain sufficient information to reconstruct the data in the event of a breach.   | Functional     | Subset Of         | 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-CMS-1-IS.1   | Media Related Records                                       | The media records must, at a minimum, contain:   | Functional     | Subset Of         | 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-CMS-1-IS.1.a | Media Related Records                                       | The name of media recipient;   | Functional     | Subset Of         | 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-CMS-1-IS.1.b | Media Related Records                                       | Signature of media recipient;  | Functional     | Subset Of         | 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-CMS-1-IS.1.c | Media Related Records                                       | Date/time media received;  | Functional     | Subset Of         | 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-CMS-1-IS.1.d | Media Related Records                                       | Media control number and contents;   | Functional     | Subset Of         | 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-CMS-1-IS.1.e | Media Related Records                                       | Movement or routing information; and   | Functional     | Subset Of         | 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-CMS-1-IS.1.f | Media Related Records                                       | If disposed of, the date, time, and method of destruction.   | Functional     | Subset Of         | 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                       |                           |
| 1.11            | Physical and Environmental Protection (PE)                  | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control |
| PE-1            | Physical and Environmental Protection Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:  | Functional     | Intersects With   | Physical Security, Compliance & Resilience Documentation              | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.   | 5                        |                           |
| PE-1            | Physical and Environmental Protection Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:  | Functional     | Subset Of         | Physical & Environmental Protections                                  | PES-01   | Mechanisms exist to facilitate the operation of physical and environmental protection controls.  | 10                       |                           |
| PE-1            | Physical and Environmental Protection Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:  | Functional     | Intersects With   | Periodic Review & Update of Security, Compliance & Resilience Program | GOV-03   | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.            | 5                        |                           |
| PE-1.a          | Physical and Environmental Protection Policy and Procedures | A formal documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  | Functional     | Subset Of         | Physical Security, Compliance & Resilience Documentation              | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.   | 10                       |                           |
| PE-1.b          | Physical and Environmental Protection Policy and Procedures | Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls   | Functional     | Subset Of         | Standardized Operating Procedures (SOP)                               | OPS-01.1 | Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day/ assigned tasks.   | 10                       |                           |
| PE-2            | Physical Access Authorizations                              | The organization:  | Functional     | Subset Of         | Physical Access Authorizations  | PES-02   | Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).                                    | 10                       |                           |
| PE-2.a          | Physical Access Authorizations                              | Develops and maintains a current list of individuals with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);  | Functional     | Subset Of         | Physical Access Authorizations  | PES-02   | Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).                                    | 10                       |                           |
| PE-2.b          | Physical Access Authorizations                              | Issues authorization credentials; and  | Functional     | Subset Of         | Physical Access Authorizations  | PES-02   | Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).                                    | 10                       |                           |
| PE-2.c          | Physical Access Authorizations                              | Reviews and approves the access list detailing authorization credentials in accordance with the frequency specified in Implementation Standard 1, removing from the access list those personnel no longer requiring access.  | Functional     | Subset Of         | Physical Access Authorizations  | PES-02   | Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).                                    | 10                       |                           |
| PE-2-5.1        | Physical Access Authorizations                              | Review and approve lists of personnel with authorized access to facilities containing information systems at least once every one hundred eighty (180) days.   | Functional     | Subset Of         | Physical Access Authorizations  | PES-02   | Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).                                    | 10                       |                           |
| PE-2-5.2        | Physical Access Authorizations                              | Create a restricted area, security room, or locked room to control access to areas containing Personally Identifiable Information (PII). These areas will be controlled accordingly.   | Functional     | Subset Of         | Physical Access Authorizations  | PES-02   | Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).                                    | 10                       |                           |
| PE-2(1)         | Access by Position / Role                                   | The organization authorizes physical access to the facility where the information system resides and information is received, processed, stored, or transmitted based on position or role.   | Functional     | Subset Of         | Role-Based Physical Access  | PES-02.1 | Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.   | 10                       |                           |
| PE-3            | Physical Access Control                                     | The organization:  | Functional     | Subset Of         | 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). | 10                       |                           |
| PE-3.a          | Physical Access Control                                     | Provides security safeguards to control access to areas within the facility officially designated as publicly accessible;  | Functional     | Subset Of         | 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). | 10                       |                           |
| PE-3.b          | Physical Access Control                                     | Escorts visitors and monitors visitor activity;  | Functional     | Subset Of         | 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). | 10                       |                           |
| PE-3.c          | Physical Access Control                                     | Enforces physical access authorizations at defined entry/exit points to the facility (defined in the applicable security plan) where the information system resides;   | Functional     | Subset Of         | 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). | 10                       |                           |
| PE-3.d          | Physical Access Control                                     | Verifies individual access authorizations before granting access to the facility;  | Functional     | Subset Of         | 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). | 10                       |                           |
| PE-3.e          | Physical Access Control                                     | Controls entry to the facility containing the information system using physical access devices/guards;   | Functional     | Subset Of         | 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). | 10                       |                           |
| PE-3.f          | Physical Access Control                                     | Maintains physical access audit logs for defined entry/exit points;  | Functional     | Subset Of         | 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). | 10                       |                           |
| PE-3.g          | Physical Access Control                                     | Secures keys, combinations, and other physical access devices;   | Functional     | Subset Of         | 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). | 10                       |                           |
| PE-3.h          | Physical Access Control                                     | Inventory physical access devices within every three hundred sixty-five (365) days; and  | Functional     | Subset Of         | 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). | 10                       |                           |
| PE-3.i          | Physical Access Control                                     | Changes combinations and keys for defined high-risk entry/exit points (defined in the applicable security plan) within every three hundred sixty-five (365) days, and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.   | Functional     | Subset Of         | 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). | 10                       |                           |
| PE-3-5.1        | Physical Access Control                                     | Control data center/facility access by use of door and window locks, and security personnel or physical authentication devices, such as biometric and/or smart card/PIN combination.   | Functional     | Subset Of         | 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). | 10                       |                           |
| PE-3-5.2        | Physical Access Control                                     | Store and operate servers in physically secure environments, and grant access to explicitly authorized personnel only. Access is monitored and recorded.   | Functional     | Subset Of         | Access To Critical Systems  | PES-03.4 | Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulatory data, in addition to the physical access controls for the facility.  | 10                       |                           |

| FDE #     | FDE Name                                  | Focal Document Element (FDE) Description  | STRM Rationale | STRM Relationship | SCF Control   | SCF #    | Secure Controls Framework (SCF) Control Description   | Strength of Relationship | Notes                     |
|-----------|---|---|----------------|-------------------|---|----------|---|--------------------------|---------------------------|
| PE-3-H.3  | Physical Access Control                   | Restrict access to grounds/facilities to authorized persons only.   | Functional     | Subset Of         | Physical Access Authorizations  | PE-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-3-H.4  | Physical Access Control                   | Require two barriers to access Personally Identifiable Information (PII) under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. Protected information must be contained in areas where other than authorized employees may have access afterhours. | Functional     | Subset Of         | Physical Access Control   | PE-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).  | 10                       |                           |
| PE-3-H.5  | Physical Access Control                   | Escort and monitor visitor activity.  | Functional     | Subset Of         | Visitor Control   | PE-06    | Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).   | 10                       |                           |
| PE-4      | Access Control for Transmission Medium    | The organization controls physical access to information system distribution and transmission lines within organizational facilities.   | Functional     | Subset Of         | Transmission Medium Security  | PE-12.1  | Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.  | 10                       |                           |
| PE-4-H.1  | Access Control for Transmission Medium    | Disable any physical ports (e.g., wiring closets and patch panels) not in use.  | Functional     | Subset Of         | Equipment Siting & Protection   | PE-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.  | 10                       |                           |
| PE-5      | Access Control for Output Devices         | The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.   | Functional     | Subset Of         | Access Control for Output Devices                                     | PE-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-6      | Monitoring Physical Access                | The organization:   | Functional     | Subset Of         | Monitoring Physical Access  | PE-05    | Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.   | 10                       |                           |
| PE-6-a    | Monitoring Physical Access                | Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;   | Functional     | Subset Of         | Monitoring Physical Access  | PE-05    | Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.   | 10                       |                           |
| PE-6-b    | Monitoring Physical Access                | Reviews physical access logs weekly and upon occurrence of security incidents involving physical security; and  | Functional     | Subset Of         | Monitoring Physical Access  | PE-05    | Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.   | 10                       |                           |
| PE-6-c    | Monitoring Physical Access                | Coordinates results of reviews and investigations with the organization's incident response capability.   | Functional     | Subset Of         | Monitoring Physical Access  | PE-05    | Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.   | 10                       |                           |
| PE-6-H.1  | Monitoring Physical Access                | The organization reviews physical access logs at least every two (2) months.  | Functional     | Subset Of         | Monitoring Physical Access  | PE-05    | Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.   | 10                       |                           |
| PE-6(H)   | Intrusion Alarms/Surveillance Equipment   | The organization monitors physical intrusion alarms and surveillance equipment.   | Functional     | Subset Of         | Intrusion Alarms / Surveillance Equipment                             | PE-05.1  | Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.   | 10                       |                           |
| PE-8      | Visitor Access Records                    | The organization:   | Functional     | Subset Of         | Physical Access Logs  | PE-03.3  | Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.   | 10                       |                           |
| PE-8-a    | Visitor Access Records                    | Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) for two (2) years; and  | Functional     | Subset Of         | Physical Access Logs  | PE-03.3  | Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.   | 10                       |                           |
| PE-8-b    | Visitor Access Records                    | Reviews visitor access records at least monthly.  | Functional     | Subset Of         | Physical Access Logs  | PE-03.3  | Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.   | 10                       |                           |
| PE-9      | Power Equipment and Cabling               | The organization protects power equipment and power cabling for the information system from damage and destruction.   | Functional     | Subset Of         | Supporting Utilities  | PE-07    | Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.   | 10                       |                           |
| PE-9-H.1  | Power Equipment and Cabling               | Permit only authorized maintenance personnel to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.  | Functional     | Subset Of         | Supporting Utilities  | PE-07    | Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.   | 10                       |                           |
| PE-10     | Emergency Shutoff                         | The organization:   | Functional     | Subset Of         | Emergency Shutoff   | PE-07.2  | Facility security mechanisms exist to shut off power in emergency situations by:(1) Placing emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel; and(2) Protecting emergency power shutoff capability from unauthorized activation. | 10                       |                           |
| PE-10-a   | Emergency Shutoff                         | Provides the capability of shutting off power to the information system or individual system components in emergency situations;  | Functional     | Subset Of         | Emergency Shutoff   | PE-07.2  | Facility security mechanisms exist to shut off power in emergency situations by:(1) Placing emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel; and(2) Protecting emergency power shutoff capability from unauthorized activation. | 10                       |                           |
| PE-10-b   | Emergency Shutoff                         | Places emergency shutoff switches or devices in a location that does not require personnel to approach the equipment to facilitate safe and easy access for personnel; and  | Functional     | Subset Of         | Emergency Shutoff   | PE-07.2  | Facility security mechanisms exist to shut off power in emergency situations by:(1) Placing emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel; and(2) Protecting emergency power shutoff capability from unauthorized activation. | 10                       |                           |
| PE-10-c   | Emergency Shutoff                         | Protects emergency power shutoff capability from unauthorized activation.   | Functional     | Subset Of         | Emergency Shutoff   | PE-07.2  | Facility security mechanisms exist to shut off power in emergency situations by:(1) Placing emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel; and(2) Protecting emergency power shutoff capability from unauthorized activation. | 10                       |                           |
| PE-11     | Emergency Power                           | The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.  | Functional     | Intersects With   | Emergency Power   | PE-07.3  | Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.   | 5                        |                           |
| PE-12     | Emergency Lighting                        | The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and covers emergency exits and evacuation routes within the facility.  | Functional     | Subset Of         | Emergency Lighting  | PE-07.4  | Facility security mechanisms exist to utilize and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.  | 10                       |                           |
| PE-13     | Fire Protection                           | The organization employs and maintains for the information system fire suppression and detection devices/systems supported by an independent energy source.   | Functional     | Subset Of         | Fire Protection   | PE-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(H)  | Detection Devices/Systems                 | The organization employs fire detection devices/systems for the information system that activate automatically and notify defined personnel (as defined in the applicable security plan) and defined emergency responders (defined in the applicable security plan) in the event of a fire.                                       | Functional     | Subset Of         | Fire Detection Devices  | PE-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(H)  | Suppression Devices/Systems               | The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to defined personnel (or roles) and defined emergency responders.  | Functional     | Intersects With   | Automatic Fire Suppression  | PE-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(H)  | Automatic Fire Suppression                | The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.  | Functional     | Intersects With   | Fire Suppression Devices  | PE-08.2  | Facility security mechanisms exist to utilize fire suppression devices/systems that provide automatic notification of any activation to organizational personnel and emergency responders.  | 5                        |                           |
| PE-14     | Temperature and Humidity Controls         | The organization:   | Functional     | Subset Of         | Temperature & Humidity Controls                                       | PE-09    | Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.   | 10                       |                           |
| PE-14-a   | Temperature and Humidity Controls         | Maintains temperature and humidity levels within the facility where the information system resides within acceptable vendor-recommended levels; and   | Functional     | Subset Of         | Temperature & Humidity Controls                                       | PE-09    | Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.   | 10                       |                           |
| PE-14-b   | Temperature and Humidity Controls         | Monitors temperature and humidity levels.   | Functional     | Subset Of         | Temperature & Humidity Controls                                       | PE-09    | Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.   | 10                       |                           |
| PE-14-H.1 | Temperature and Humidity Controls         | Evaluate the level of alert and follow prescribed guidelines for that alert level.  | Functional     | Subset Of         | Temperature & Humidity Controls                                       | PE-09    | Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.   | 10                       |                           |
| PE-14-H.2 | Temperature and Humidity Controls         | Alert component management of possible loss of service and/or media.  | Functional     | Subset Of         | Temperature & Humidity Controls                                       | PE-09    | Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.   | 10                       |                           |
| PE-14-H.3 | Temperature and Humidity Controls         | Report damage and provide remedial action. Implement contingency plan, if necessary.  | Functional     | Subset Of         | Temperature & Humidity Controls                                       | PE-09    | Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.   | 10                       |                           |
| PE-15     | Water Damage Protection                   | The organization protects the information 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     | Subset Of         | Water Damage Protection   | PE-07.5  | Facility security mechanisms exist to protect systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly and known to key personnel.   | 10                       |                           |
| PE-16     | Delivery and Removal                      | The organization authorizes, monitors, and controls the flow of information system-related components entering and exiting the facility and maintains records of those items.   | Functional     | Subset Of         | Delivery & Removal  | PE-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-H.1 | Delivery and Removal                      | The organization authorizes, monitors, and controls the flow of all information system components entering and exiting the facility and maintains records of those items.   | Functional     | Subset Of         | Delivery & Removal  | PE-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-17     | Alternate Work Site                       | The organization:   | Functional     | Subset Of         | Alternate Work Site   | PE-11    | Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.   | 10                       |                           |
| PE-17-a   | Alternate Work Site                       | Employs appropriate security controls at alternate work sites that include, but are not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems at alternate work sites.  | Functional     | Subset Of         | Alternate Work Site   | PE-11    | Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.   | 10                       |                           |
| PE-17-b   | Alternate Work Site                       | Assesses as feasible, the effectiveness of security controls at alternate work sites; and   | Functional     | Subset Of         | Alternate Work Site   | PE-11    | Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.   | 10                       |                           |
| PE-17-c   | Alternate Work Site                       | Provides a means for employees to communicate with information security personnel in case of security incidents or problems.  | Functional     | Subset Of         | Alternate Work Site   | PE-11    | Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.   | 10                       |                           |
| PE-17-H.1 | Alternate Work Site                       | The organization defines management, operational, and technical information system security controls for alternate work sites.  | Functional     | Subset Of         | Alternate Work Site   | PE-11    | Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.   | 10                       |                           |
| PE-18     | Location of Information System Components | The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards, and to minimize the opportunity for unauthorized access.   | Functional     | Intersects With   | Equipment Siting & Protection   | PE-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                        |                           |
| 1.12      | Planning (PL)                             | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A   | 0                        | No applicable SCF control |
| PL-1      | Security Planning Policy and Procedures   | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:   | Functional     | Subset Of         | Security, Compliance & Resilience Protection Portfolio Management     | PRM-01   | Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.   | 10                       |                           |
| PL-1      | Security Planning Policy and Procedures   | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:   | Functional     | Subset Of         | Statutory, Regulatory & Contractual Compliance                        | CPL-01   | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.  | 10                       |                           |
| PL-1      | Security Planning Policy and Procedures   | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:   | Functional     | Subset Of         | Technology Development & Acquisition                                  | TDA-01   | Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.   | 10                       |                           |
| PL-1      | Security Planning Policy and Procedures   | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:   | Functional     | Intersects With   | Periodic Review & Update of Security, Compliance & Resilience Program | GOV-03   | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.   | 5                        |                           |
| PL-1      | Security Planning Policy and Procedures   | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:   | Functional     | Intersects With   | Publishing Security, Compliance & Resilience Documentation            | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.  | 5                        |                           |
| PL-1-a    | Security Planning Policy and Procedures   | A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and   | Functional     | Subset Of         | Publishing Security, Compliance & Resilience Documentation            | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.  | 10                       |                           |
| PL-1-b    | Security Planning Policy and Procedures   | Procedures to facilitate the implementation of the security planning policy and associated security planning controls.  | Functional     | Subset Of         | Standardized Operating Procedures (SOP)                               | OPS-01.1 | Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.   | 10                       |                           |
| PL-2      | System Security Plan                      | The organization:   | 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                        |                           |



| FDE #     | FDE Name                                 | Focal Document Element (FDE) Description   | STRM Rationale | STRM Relationship | SCF Control   | SCF #    | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes                     |
|-----------|--|--|----------------|-------------------|---|----------|--|--------------------------|---------------------------|
| PL-8      | Information Security Architecture        | The organization:  | Functional     | Subset Of         | Alignment With Enterprise Architecture                                | SEA-02   | Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations. | 10                       |                           |
| PL-8.a    | Information Security Architecture        | Develops an information security architecture for the ACA system that:   | Functional     | Subset Of         | Alignment With Enterprise Architecture                                | SEA-02   | Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations. | 10                       |                           |
| PL-8.a.1  | Information Security Architecture        | Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.   | Functional     | Subset Of         | Alignment With Enterprise Architecture                                | SEA-02   | Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations. | 10                       |                           |
| PL-8.a.2  | Information Security Architecture        | Describes how the information security architecture is integrated into and supports the enterprise architecture.   | Functional     | Subset Of         | Alignment With Enterprise Architecture                                | SEA-02   | Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations. | 10                       |                           |
| PL-8.a.3  | Information Security Architecture        | Describes any information security assumptions about, and dependencies on, external services.  | Functional     | Subset Of         | Alignment With Enterprise Architecture                                | SEA-02   | Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations. | 10                       |                           |
| PL-8.b    | Information Security Architecture        | Reviews and updates (as necessary) the information security architecture whenever changes are made to the enterprise architecture; and   | Functional     | Subset Of         | Alignment With Enterprise Architecture                                | SEA-02   | Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations. | 10                       |                           |
| PL-8.c    | Information Security Architecture        | Ensures that planned information security architecture changes are reflected in the security plan and organizational procurements/acquisitions.  | Functional     | Subset Of         | Alignment With Enterprise Architecture                                | SEA-02   | Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations. | 10                       |                           |
| 1.13      | Personnel Security (PS)                  | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control |
| PS-1      | Personnel Security Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:  | Functional     | Intersects With   | Publishing Security, Compliance & Resilience Documentation            | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.   | 5                        |                           |
| PS-1      | Personnel Security Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:  | Functional     | Intersects With   | Periodic Review & Update of Security, Compliance & Resilience Program | GOV-03   | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRIP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.                         | 5                        |                           |
| PS-1      | Personnel Security Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:  | Functional     | Subset Of         | Human Resources Security Management                                   | HRS-01   | Mechanisms exist to facilitate the implementation of personnel security controls.  | 10                       |                           |
| PS-1.a    | Personnel Security Policy and Procedures | A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and   | Functional     | Subset Of         | Publishing Security, Compliance & Resilience Documentation            | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.   | 10                       |                           |
| PS-1.b    | Personnel Security Policy and Procedures | Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.   | Functional     | Subset Of         | Standardized Operating Procedures (SOP)                               | OPS-01.1 | Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.  | 10                       |                           |
| PS-2      | Position Risk Designation                | The organization:  | Functional     | Intersects With   | Competency Requirements for Security-Related Positions                | HRS-03.2 | Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.  | 5                        |                           |
| PS-2      | Position Risk Designation                | The organization:  | Functional     | Subset Of         | 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.   | 10                       |                           |
| PS-2.a    | Position Risk Designation                | Assigns a criticality/sensitivity risk designation to all organizational positions;  | Functional     | Subset Of         | 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.   | 10                       |                           |
| PS-2.b    | Position Risk Designation                | Establishes screening criteria for individuals filling those positions; and  | Functional     | Subset Of         | 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.   | 10                       |                           |
| PS-2.c    | Position Risk Designation                | Reviews and revises position criticality/sensitivity risk designations within every three hundred sixty-five (365) days.   | Functional     | Subset Of         | 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.   | 10                       |                           |
| PS-3      | Personnel Screening                      | The organization:  | Functional     | Subset Of         | Personnel Screening   | HRS-04   | Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.   | 10                       |                           |
| PS-3.a    | Personnel Screening                      | Screens individuals prior to authorizing access to the information system:   | Functional     | Subset Of         | Personnel Screening   | HRS-04   | Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.   | 10                       |                           |
| PS-3.b    | Personnel Screening                      | Rescreens individuals periodically, consistent with the criticality/sensitivity risk designation of the position; and  | Functional     | Subset Of         | Personnel Screening   | HRS-04   | Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.   | 10                       |                           |
| PS-3.c    | Personnel Screening                      | When an employee moves from one position to another, the higher level of clearance should be adjudicated.  | Functional     | Subset Of         | Personnel Screening   | HRS-04   | Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.   | 10                       |                           |
| PS-3-IS.1 | Personnel Screening                      | Perform criminal history check for all persons prior to employment.  | Functional     | Subset Of         | Personnel Screening   | HRS-04   | Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.   | 10                       |                           |
| PS-3-IS.2 | Personnel Screening                      | All employees and contractors requiring access to ACA-sensitive information must meet personnel suitability standards. These suitability standards are based on a valid need-to-know, which cannot be assumed from position or title, and favorable results from a background check. The background check for prospective and existing employees (if not previously completed) should include, at a minimum, contacting references provided by the employee as well as the local law enforcement agency or agencies. | Functional     | Subset Of         | Personnel Screening   | HRS-04   | Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.   | 10                       |                           |
| PS-4      | Personnel Termination                    | The organization, upon termination of individual employment:   | Functional     | Subset Of         | Personnel Termination   | HRS-09   | Mechanisms exist to govern the termination of individual employment.   | 10                       |                           |
| PS-4.a    | Personnel Termination                    | Disables information system access in accordance with Implementation Standard 1;   | Functional     | Subset Of         | Personnel Termination   | HRS-09   | Mechanisms exist to govern the termination of individual employment.   | 10                       |                           |
| PS-4.b    | Personnel Termination                    | Terminates/revokes any authenticators/credentials associated with the individual;  | Functional     | Subset Of         | Personnel Termination   | HRS-09   | Mechanisms exist to govern the termination of individual employment.   | 10                       |                           |
| PS-4.c    | Personnel Termination                    | Conducts exit interviews that include a discussion of non-disclosure of information security and privacy information;  | Functional     | Subset Of         | Personnel Termination   | HRS-09   | Mechanisms exist to govern the termination of individual employment.   | 10                       |                           |
| PS-4.d    | Personnel Termination                    | Retrieves all security-related organizational information system-related property;   | Functional     | Subset Of         | Personnel Termination   | HRS-09   | Mechanisms exist to govern the termination of individual employment.   | 10                       |                           |
| PS-4.e    | Personnel Termination                    | Retains access to organizational information and information systems formerly controlled by a terminated individual;   | Functional     | Subset Of         | Personnel Termination   | HRS-09   | Mechanisms exist to govern the termination of individual employment.   | 10                       |                           |
| PS-4.f    | Personnel Termination                    | Notifies defined personnel or roles (defined in the applicable security plan) within one (1) business day; and   | Functional     | Subset Of         | Personnel Termination   | HRS-09   | Mechanisms exist to govern the termination of individual employment.   | 10                       |                           |
| PS-4.g    | Personnel Termination                    | Immediately escorts employees terminated for cause out of the organization.  | Functional     | Subset Of         | Personnel Termination   | HRS-09   | Mechanisms exist to govern the termination of individual employment.   | 10                       |                           |
| PS-4-IS.1 | Personnel Termination                    | System and physical access must be revoked prior to or during the employee termination process.  | Functional     | Subset Of         | Personnel Termination   | HRS-09   | Mechanisms exist to govern the termination of individual employment.   | 10                       |                           |
| PS-4-IS.2 | Personnel Termination                    | All access and privileges to systems, networks, and facilities are suspended when employees or contractors temporarily separate from the organization (e.g., leave of absence).  | Functional     | Subset Of         | Personnel Termination   | HRS-09   | Mechanisms exist to govern the termination of individual employment.   | 10                       |                           |
| PS-5      | Personnel Transfer                       | The organization:  | Functional     | Subset Of         | Personnel Transfer  | HRS-08   | Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.  | 10                       |                           |
| PS-5.a    | Personnel Transfer                       | Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;  | Functional     | Subset Of         | Personnel Transfer  | HRS-08   | Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.  | 10                       |                           |
| PS-5.b    | Personnel Transfer                       | Initiates the following transfer or reassignment actions during the formal transfer process:   | Functional     | Subset Of         | Personnel Transfer  | HRS-08   | Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.  | 10                       |                           |
| PS-5.b.1  | Personnel Transfer                       | Re-issuing appropriate information system-related property (e.g., keys, identification cards, and building passes);  | Functional     | Subset Of         | Personnel Transfer  | HRS-08   | Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.  | 10                       |                           |
| PS-5.b.2  | Personnel Transfer                       | Notification to security management;   | Functional     | Subset Of         | Personnel Transfer  | HRS-08   | Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.  | 10                       |                           |
| PS-5.b.3  | Personnel Transfer                       | Closing obsolete accounts and establishing new accounts;   | Functional     | Subset Of         | Personnel Transfer  | HRS-08   | Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.  | 10                       |                           |
| PS-5.b.4  | Personnel Transfer                       | When an employee moves to a new position of trust, logical and physical access controls must be reevaluated as soon as possible but not to exceed thirty (30) days;  | Functional     | Subset Of         | Personnel Transfer  | HRS-08   | Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.  | 10                       |                           |
| PS-5.c    | Personnel Transfer                       | Modifies access authorization as necessary to correspond with any changes in operational need due to reassignment or transfer; and   | Functional     | Subset Of         | Personnel Transfer  | HRS-08   | Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.  | 10                       |                           |
| PS-5.d    | Personnel Transfer                       | Notifies defined personnel or roles (defined in the applicable security plan) within one (1) business day.   | Functional     | Subset Of         | 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-6      | Access Agreements                        | The organization:  | Functional     | Intersects With   | Confidentiality Agreements  | HRS-06.1 | Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.  | 5                        |                           |
| PS-6      | Access Agreements                        | The organization:  | Functional     | Subset Of         | Access Agreements   | HRS-06   | Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.  | 10                       |                           |
| PS-6.a    | Access Agreements                        | Develops and documents access agreements for organizational information systems, consistent with the provisions of the ACA and the requirements of 45 CFR 135.260 - Privacy and security of personally identifiable information, paragraphs (b)(2) and (c).  | Functional     | Subset Of         | Access Agreements   | HRS-06   | Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.  | 10                       |                           |
| PS-6.b    | Access Agreements                        | Reviews and updates the access agreements as part of the system security authorization or when a contract is renewed or extended, but minimally within every three hundred sixty-five (365) days, whichever occurs first; and  | Functional     | Subset Of         | Access Agreements   | HRS-06   | Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.  | 10                       |                           |
| PS-6.c    | Access Agreements                        | Ensures that individuals requiring access to organizational information and information systems:   | Functional     | Subset Of         | Access Agreements   | HRS-06   | Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.  | 10                       |                           |
| PS-6.c.1  | Access Agreements                        | Acknowledge (paper or electronic) appropriate access agreements prior to being granted access; and   | Functional     | Subset Of         | Access Agreements   | HRS-06   | Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.  | 10                       |                           |
| PS-6.c.2  | Access Agreements                        | Re-acknowledge access agreements to maintain access to organizational information systems when access agreements have been updated.  | Functional     | Subset Of         | Access Agreements   | HRS-06   | Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.  | 10                       |                           |
| PS-7      | Third-Party Personnel Security           | The organization:  | Functional     | Subset Of         | Third-Party Personnel   | HRS-10   | Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party security, compliance and/or resilience roles and responsibilities.  | 10                       |                           |
| PS-7.a    | Third-Party Personnel Security           | Establishes personnel security requirements including security roles and responsibilities for third-party providers;   | Functional     | Subset Of         | Third-Party Personnel   | HRS-10   | Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party security, compliance and/or resilience roles and responsibilities.  | 10                       |                           |
| PS-7.b    | Third-Party Personnel Security           | Requires third-party providers to comply with personnel security policies and procedures established by the organization;  | Functional     | Subset Of         | Third-Party Personnel   | HRS-10   | Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party security, compliance and/or resilience roles and responsibilities.  | 10                       |                           |
| PS-7.c    | Third-Party Personnel Security           | Documents personnel security requirements;   | Functional     | Subset Of         | Third-Party Personnel   | HRS-10   | Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party security, compliance and/or resilience roles and responsibilities.  | 10                       |                           |

| FDE #    | FDE Name  | Focal Document Element (FDE) Description   | STRM Rationale | STRM Relationship | SCF Control   | SCF #    | Secure Controls Framework (SCF) Control Description   | Strength of Relationship | Notes                     |
|----------|---|--|----------------|-------------------|---|----------|---|--------------------------|---------------------------|
| PS-7.d   | Third-Party Personnel Security                        | Requires third-party providers to notify Contracting Officers or Contracting Officers' Representatives (via the roster of contractor personnel) of any personnel transfers or terminations of third-party personnel who possess organizational information, or who have information system privileges within fifteen (15) calendar days; and   | Functional     | Subset Of         | Third-Party Personnel   | HRS-10   | Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party security, compliance and/or resilience roles and responsibilities.   | 10                       |                           |
| PS-7.e   | Third-Party Personnel Security                        | Monitors provider compliance.  | Functional     | Subset Of         | Third-Party Personnel   | HRS-10   | Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party security, compliance and/or resilience roles and responsibilities.   | 10                       |                           |
| PS-7-5.1 | Third-Party Personnel Security                        | Regulate the access provided to contractors and define security requirements for contractors. Contractors must be provided with minimal system and physical access, and must agree to and support the information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support information security policies and standards.                                 | Functional     | Subset Of         | Third-Party Personnel   | HRS-10   | Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party security, compliance and/or resilience roles and responsibilities.   | 10                       |                           |
| PS-8     | Personnel Sanctions                                   | The organization:  | Functional     | Subset Of         | Personnel Sanctions   | HRS-07   | Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.  | 10                       |                           |
| PS-8.a   | Personnel Sanctions                                   | Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and  | Functional     | Subset Of         | Personnel Sanctions   | HRS-07   | Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.  | 10                       |                           |
| PS-8.b   | Personnel Sanctions                                   | Notifies defined personnel or roles (defined in the applicable security plan) within defined time period (defined in the applicable security plan) when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.   | Functional     | Subset Of         | Personnel Sanctions   | HRS-07   | Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.  | 10                       |                           |
| 1.14     | Risk Assessment (RA)                                  | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A   | 0                        | No applicable SCF control |
| RA-1     | Risk Assessment Policy and Procedure                  | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as applicable) within every three hundred sixty-five (365) days   | Functional     | Intersects With   | Periodic Review & Update of Security, Compliance & Resilience Program | GOV-03   | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.   | 5                        |                           |
| RA-1     | Risk Assessment Policy and Procedure                  | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as applicable) within every three hundred sixty-five (365) days;  | Functional     | Subset Of         | Risk Management Program   | RSK-01   | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.  | 10                       |                           |
| RA-1     | Risk Assessment Policy and Procedure                  | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as applicable) within every three hundred sixty-five (365) days;  | Functional     | Intersects With   | Publishing Security, Compliance & Resilience Documentation            | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.  | 5                        |                           |
| RA-1.a   | Risk Assessment Policy and Procedure                  | A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and   | Functional     | Subset Of         | Risk Management Program   | RSK-01   | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.  | 10                       |                           |
| RA-1.b   | Risk Assessment Policy and Procedure                  | Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.  | Functional     | Subset Of         | Risk Management Program   | RSK-01   | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.  | 10                       |                           |
| RA-2     | Security Categorization                               | The organization:  | Functional     | Subset Of         | 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-2.a   | Security Categorization                               | Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.   | Functional     | Subset Of         | 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-2.b   | Security Categorization                               | Documents the security categorization results (including supporting rationale) in the security plan for the information system; and  | Functional     | Subset Of         | 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-2.e   | Security Categorization                               | Ensures the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.  | Functional     | Subset Of         | 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-3     | Risk Assessment                                       | The organization:  | Functional     | Intersects With   | Functional Review Of Security, Compliance & Resilience Controls       | CPL-03.2 | Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.  | 5                        |                           |
| RA-3     | Risk Assessment                                       | The organization:  | Functional     | Subset Of         | Risk Assessment   | RSK-04   | Mechanisms exist to conduct recurring assessments of risk that include 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).  | 10                       |                           |
| RA-3.a   | Risk Assessment                                       | Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;  | Functional     | Subset Of         | Risk Assessment   | RSK-04   | Mechanisms exist to conduct recurring assessments of risk that include 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).  | 10                       |                           |
| RA-3.b   | Risk Assessment                                       | Documents risk assessment results in the applicable security plan;   | Functional     | Subset Of         | Risk Assessment   | RSK-04   | Mechanisms exist to conduct recurring assessments of risk that include 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).  | 10                       |                           |
| RA-3.c   | Risk Assessment                                       | Reviews risk assessment results within every three hundred sixty-five (365) days;  | Functional     | Subset Of         | Risk Assessment   | RSK-04   | Mechanisms exist to conduct recurring assessments of risk that include 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).  | 10                       |                           |
| RA-3.d   | Risk Assessment                                       | Disseminates risk assessment results to affected stakeholders, Business Owners(s), and CMS; and  | Functional     | Subset Of         | Risk Assessment   | RSK-04   | Mechanisms exist to conduct recurring assessments of risk that include 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).  | 10                       |                           |
| RA-3.e   | Risk Assessment                                       | Updates the risk assessment every three (3) years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system. Significant change is defined in NIST Special Publication 800-37 Revision 1, Section F.4 of Appendix F.) | Functional     | Subset Of         | Risk Assessment   | RSK-04   | Mechanisms exist to conduct recurring assessments of risk that include 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).  | 10                       |                           |
| RA-3-5.1 | Risk Assessment                                       | The organization conducts an information security risk assessment and documents risk assessment results in the security assessment report template that is found at: <a href="https://cait.cms.gov/ds/projects/cms_aca_program_security_privacy/">https://cait.cms.gov/ds/projects/cms_aca_program_security_privacy/</a> .   | Functional     | Subset Of         | Risk Assessment   | RSK-04   | Mechanisms exist to conduct recurring assessments of risk that include 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).  | 10                       |                           |
| RA-3-5.2 | Risk Assessment                                       | The system owner reviews risk assessment results at least every three hundred sixty-five (365) days or when a significant change occurs.   | Functional     | Subset Of         | Risk Assessment   | RSK-04   | Mechanisms exist to conduct recurring assessments of risk that include 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).  | 10                       |                           |
| RA-5     | Vulnerability Scanning                                | The organization:  | Functional     | Subset Of         | Vulnerability Scanning  | VPM-06   | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.  | 10                       |                           |
| RA-5     | Vulnerability Scanning                                | The organization:  | Functional     | Intersects With   | Update Tool Capability  | VPM-06.1 | Mechanisms exist to update vulnerability scanning tools.  | 5                        |                           |
| RA-5.a   | Vulnerability Scanning                                | Scans for vulnerabilities in the information system and hosted applications, operating system, web application, and database scans (as applicable) within every thirty (30) days and when new vulnerabilities potentially affecting the system/applications are identified and reported ;  | Functional     | Subset Of         | Vulnerability Scanning  | VPM-06   | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.  | 10                       |                           |
| RA-5.b   | Vulnerability Scanning                                | Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for;  | Functional     | Subset Of         | Vulnerability Scanning  | VPM-06   | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.  | 10                       |                           |
| RA-5.b.1 | Vulnerability Scanning                                | Enumerating platforms, software flaws, and improper configurations;  | Functional     | Subset Of         | Vulnerability Scanning  | VPM-06   | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.  | 10                       |                           |
| RA-5.b.2 | Vulnerability Scanning                                | Formatting checklists and test procedures;   | Functional     | Subset Of         | Vulnerability Scanning  | VPM-06   | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.  | 10                       |                           |
| RA-5.b.3 | Vulnerability Scanning                                | Measuring vulnerability impact;  | Functional     | Subset Of         | Vulnerability Scanning  | VPM-06   | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.  | 10                       |                           |
| RA-5.c   | Vulnerability Scanning                                | Analyzes vulnerability scan reports and results from security control assessments;   | Functional     | Subset Of         | Vulnerability Scanning  | VPM-06   | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.  | 10                       |                           |
| RA-5.d   | Vulnerability Scanning                                | Remediates legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational assessment of risk; and   | Functional     | Subset Of         | Vulnerability Scanning  | VPM-06   | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.  | 10                       |                           |
| RA-5.e   | Vulnerability Scanning                                | Shares information obtained from the vulnerability scanning process and security control assessments with affected related stakeholders on a "need to know" basis to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).  | Functional     | Subset Of         | Vulnerability Scanning  | VPM-06   | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.  | 10                       |                           |
| RA-5-5.1 | Vulnerability Scanning                                | Perform external network penetration testing and conduct enterprise security posture reviews as needed but no less than once within every three hundred sixty-five (365) days, in accordance with organizational Information Security procedures.  | Functional     | Subset Of         | Vulnerability Scanning  | VPM-06   | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.  | 10                       |                           |
| RA-5-5.2 | Vulnerability Scanning                                | Legitimate high-risk vulnerabilities are mitigated within thirty (30) days, and moderate risk vulnerabilities are mitigated within ninety (90) days.   | Functional     | Subset Of         | Vulnerability Scanning  | VPM-06   | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.  | 10                       |                           |
| RA-5(1)  | Update Tool Capability                                | The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities scanned.  | Functional     | Subset Of         | Vulnerability Scanning  | VPM-06   | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.  | 10                       |                           |
| RA-5(2)  | Update by Frequency/Prior to New Scan/When Identified | The organization updates the information system vulnerabilities scanned within every thirty (30) days or 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-5(3)  | Breadth/Depth of Coverage                             | The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).   | Functional     | Subset Of         | Breadth / Depth of Coverage   | VPM-06.2 | Mechanisms exist to identify the breadth and depth of coverage for vulnerability scanning that define the system components scanned and types of vulnerabilities that are checked for.  | 10                       |                           |
| RA-5(5)  | Privileged Access                                     | The information system implements privileged access authorization to operating system, telecommunications, and configuration components for selected vulnerability scanning activities to facilitate more thorough scanning.   | Functional     | Subset Of         | Privileged Access   | VPM-06.3 | Mechanisms exist to implement privileged access authorization for selected vulnerability scanning activities.   | 10                       |                           |
| 1.15     | System and Services Acquisition (SA)                  | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A   | 0                        | No applicable SCF control |
| SA-1     | System and Services Acquisition Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as applicable), within every three hundred sixty-five (365) days;   | Functional     | Intersects With   | Publishing Security, Compliance & Resilience Documentation            | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.  | 5                        |                           |
| SA-1     | System and Services Acquisition Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as applicable), within every three hundred sixty-five (365) days;   | 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                       |                           |

| FDE #      | FDE Name  | Focal Document Element (FDE) Description  | STRM Rationale | STRM Relationship | SCF Control   | SCF #    | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes |
|------------|---|---|----------------|-------------------|---|----------|--|--------------------------|-------|
| SA-1       | System and Services Acquisition Policy and Procedures   | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as applicable), within every three hundred sixty-five (365) days:  | Functional     | Intersects With   | Periodic Review & Update of Security, Compliance & Resilience Program | GOV-03   | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.  | 5                        |       |
| SA-1       | System and Services Acquisition Policy and Procedures   | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as applicable), within every three hundred sixty-five (365) days:  | Functional     | Intersects With   | Secure Software Development Practices (SSDP)                          | TDA-06   | Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).  | 5                        |       |
| SA-1.a     | System and Services Acquisition Policy and Procedures   | A formal documented system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and   | Functional     | Subset Of         | Publishing Security, Compliance & Resilience Program                  | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.   | 10                       |       |
| SA-1.b     | System and Services Acquisition Policy and Procedures   | Formal documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.  | Functional     | Subset Of         | Standardized Operating Procedures (SOP)                               | OPS-01.1 | Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.  | 10                       |       |
| SA-2       | Allocation of Resources                                 | The organization:   | Functional     | Subset Of         | 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-2.a     | Allocation of Resources                                 | Determines information security requirements for the information system or information system service in mission/business process planning;   | Functional     | Subset Of         | 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-2.b     | Allocation of Resources                                 | Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process.   | Functional     | Subset Of         | 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-2.c     | Allocation of Resources                                 | Includes information security requirements in mission/business case planning, and   | Functional     | Subset Of         | 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-2.d     | Allocation of Resources                                 | Establishes a discrete line item in programming and budgeting documentation for the implementation and management of information systems security.  | Functional     | Subset Of         | 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-3       | System Development Life Cycle                           | The organization:   | 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-3       | System Development Life Cycle                           | The organization:   | Functional     | Subset Of         | 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.  | 10                       |       |
| SA-3.a     | System Development Life Cycle                           | Manages the information system using the organization-defined system development life cycle (SDLC) that incorporates information security considerations;   | Functional     | Subset Of         | 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.  | 10                       |       |
| SA-3.b     | System Development Life Cycle                           | Defines and documents information security roles and responsibilities throughout the system development life cycle;   | Functional     | Subset Of         | 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.  | 10                       |       |
| SA-3.c     | System Development Life Cycle                           | Identifies individuals having information system security roles and responsibilities; and   | Functional     | Subset Of         | 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.  | 10                       |       |
| SA-3.d     | System Development Life Cycle                           | Integrates the organizational information security risk management process into system development life cycle activities.   | Functional     | Subset Of         | 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.  | 10                       |       |
| SA-4       | Acquisition Process                                     | The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:  | 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-4       | Acquisition Process                                     | The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:  | Functional     | Intersects With   | Third-Party Management  | TPM-01   | Mechanisms exist to facilitate the implementation of third-party management controls.  | 5                        |       |
| SA-4       | Acquisition Process                                     | The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:  | 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-4       | Acquisition Process                                     | The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:  | 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-4.a     | Acquisition Process                                     | Security functional requirements;   | 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-4.b     | Acquisition Process                                     | Security strength requirements;   | 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-4.c     | Acquisition Process                                     | Security assurance requirements;  | 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-4.d     | Acquisition Process                                     | Security-related documentation requirements;  | 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-4.e     | Acquisition Process                                     | Requirements for protecting security-related documentation;   | 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-4.f     | Acquisition Process                                     | Description of the information system development environment and environment in which the system is intended to operate;   | 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-4.g     | Acquisition Process                                     | Acceptance criteria; and  | 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-4.h     | Acquisition Process                                     | Requirement that providers of defined external information systems identify the location of information systems that receive, process, store, or transmit data.   | 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-4.i.1   | Acquisition Process                                     | Each contract and Statement of Work (SOW) that requires development or access to systems that contain Personally Identifiable Information (PII) must include language requiring adherence to the security and privacy policies and standards set by the organization consistent with 45 CFR 1155.260(b); define security and privacy roles and responsibilities; and receive approval from the system owner.  | 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-4.i.2   | Acquisition Process                                     | When contracting with external service providers:   | 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-4.i.2.a | Acquisition Process                                     | As part of the service contract, the AE must establish security and privacy policies and procedures for how data is stored, handled, and accessed within service provider environment;  | 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-4.i.2.b | Acquisition Process                                     | The data must be encrypted in transit to and from the service provider environment;   | 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-4.i.2.c | Acquisition Process                                     | All mechanisms used to encrypt data must be FIPS 140-2 compliant, and operate using the FIPS 140-2 compliant module; and  | 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-4.i.2.d | Acquisition Process                                     | Storage devices where data has resided must be securely sanitized according to NIST SP 800-88 Media Sanitization security control prior to use.   | 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-4.i.2.e | Acquisition Process                                     | Per SA-9 (5), the outsourcing of information system services outside the continental U.S. must be authorized by the CIO of CMS.   | 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-4(1)    | Functional Properties of Security Controls              | The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.   | Functional     | Intersects With   | Functional Properties   | TDA-04.1 | Mechanisms exist to require software developers to provide information describing the functional properties of the security, compliance and resilience controls to be utilized within Technology Assets, Applications and/or Services (TAAS) in sufficient detail to permit analysis and testing of the controls.          | 5                        |       |
| SA-4(1)    | Functional Properties of Security Controls              | The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.   | 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/regulate data flows.   | 5                        |       |
| SA-4(2)    | Design/Implementation Information for Security Controls | The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed, which shall include security-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces and high-level design documentation at sufficient detail to prove the security control implementation. | 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/regulate data flows.   | 5                        |       |
| SA-4(2)    | Design/Implementation Information for Security Controls | The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed, which shall include security-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces and high-level design documentation at sufficient detail to prove the security control implementation. | Functional     | Intersects With   | Access to Program Source Code   | TDA-20   | Mechanisms exist to limit privileges to change software resident within software libraries.  | 5                        |       |
| SA-4(2)    | Design/Implementation Information for Security Controls | The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed, which shall include security-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces and high-level design documentation at sufficient detail to prove the security control implementation. | Functional     | Intersects With   | Functional Properties   | TDA-04.1 | Mechanisms exist to require software developers to provide information describing the functional properties of the security, compliance and resilience controls to be utilized within Technology Assets, Applications and/or Services (TAAS) in sufficient detail to permit analysis and testing of the controls.          | 5                        |       |
| SA-4(9)    | Functions/Ports/Protocols Services in Use               | The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle the functions, ports, protocols, and services intended for organizational use.  | Functional     | Subset Of         | 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                       |       |

| FDE #        | FDE Name   | Focal Document Element (FDE) Description  | STRM Rationale | STRM Relationship | SCF Control   | SCF #    | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes |
|--------------|--|---|----------------|-------------------|---|----------|--|--------------------------|-------|
| SA-5         | Information System Documentation                     | The organization:   | Functional     | Subset Of         | 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. | 10                       |       |
| SA-5         | Information System Documentation                     | The organization:   | Functional     | Intersects With   | Asset Scope Classification  | AST-04.1 | Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and documenting the appropriate asset scope category for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).  | 5                        |       |
| SA-5.a       | Information System Documentation                     | Obtains administrator documentation for the information system, system component, or information system service that describes:   | Functional     | Subset Of         | 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. | 10                       |       |
| SA-5.a.1     | Information System Documentation                     | Secure configuration, installation, and operation of the system, component, or service;   | Functional     | Subset Of         | 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. | 10                       |       |
| SA-5.a.2     | Information System Documentation                     | Effective use and maintenance of security functions/mechanisms; and   | Functional     | Subset Of         | 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. | 10                       |       |
| SA-5.a.3     | Information System Documentation                     | Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;   | Functional     | Subset Of         | 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. | 10                       |       |
| SA-5.b       | Information System Documentation                     | Obtains user documentation for the information system, system component, or information system service that describes:  | Functional     | Subset Of         | 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. | 10                       |       |
| SA-5.b.1     | Information System Documentation                     | User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;   | Functional     | Subset Of         | 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. | 10                       |       |
| SA-5.b.2     | Information System Documentation                     | Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and   | Functional     | Subset Of         | 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. | 10                       |       |
| SA-5.b.3     | Information System Documentation                     | User responsibilities in maintaining the security of the system, component, or service;   | Functional     | Subset Of         | 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. | 10                       |       |
| SA-5.c       | Information System Documentation                     | Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.   | Functional     | Subset Of         | 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. | 10                       |       |
| SA-5-IS.1    | Information System Documentation                     | Develop system documentation to describe the system and to specify the purpose, technical operation, access, maintenance, and required training for administrators and users.   | Functional     | Subset Of         | 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. | 10                       |       |
| SA-5-IS.2    | Information System Documentation                     | Maintain an updated list of related system operations and security documentation.   | Functional     | Subset Of         | 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. | 10                       |       |
| SA-5-IS.3    | Information System Documentation                     | Update documentation upon changes in system functions and processes.  | Functional     | Subset Of         | 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. | 10                       |       |
| SA-5-IS.4    | Information System Documentation                     | Must include date and version number on all formal system documentation.  | Functional     | Subset Of         | 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. | 10                       |       |
| SA-8         | Security Engineering                                 | The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.  | Functional     | Intersects With   | Secure Baseline Configurations  | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 5                        |       |
| SA-8         | Security Engineering                                 | The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.  | Functional     | Intersects With   | Secure Engineering Principles   | SEA-01   | Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).   | 5                        |       |
| SA-9         | External Information System Services                 | The organization:   | Functional     | Subset Of         | Third-Party Services  | TPM-04   | Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).   | 10                       |       |
| SA-9.a       | External Information System Services                 | Must notify CMS of plans to outsource information system services prior to the awarding of contract. Per SA-9 (5), the outsourcing of information system services outside the continental U.S. must be authorized by the CIO of CMS.  | Functional     | Subset Of         | Third-Party Services  | TPM-04   | Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).   | 10                       |       |
| SA-9.b       | External Information System Services                 | Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. | Functional     | Subset Of         | Third-Party Services  | TPM-04   | Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).   | 10                       |       |
| SA-9.c       | External Information System Services                 | Defines and documents oversight and user roles and responsibilities with regard to external information system services.  | Functional     | Subset Of         | Third-Party Services  | TPM-04   | Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).   | 10                       |       |
| SA-9.d       | External Information System Services                 | Ensures that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instances of noncompliance; and  | Functional     | Subset Of         | Third-Party Services  | TPM-04   | Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).   | 10                       |       |
| SA-9.e       | External Information System Services                 | Employs defined processes, methods, and techniques (defined in the applicable security plan) to monitor security and privacy control compliance by external service providers on an ongoing basis.  | Functional     | Subset Of         | Third-Party Services  | TPM-04   | Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).   | 10                       |       |
| SA-9-IS.1    | External Information System Services                 | The service contract or agreement must include language requiring the provider to be subject to U.S. Federal laws and regulations protecting PII.   | Functional     | Subset Of         | Third-Party Services  | TPM-04   | Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).   | 10                       |       |
| SA-9-IS.2    | External Information System Services                 | The service contract or agreement must include language requiring adherence to the security and privacy policies and standards set by the organization consistent with 45 CFR 155.260(b), define security and privacy roles and responsibilities.   | Functional     | Subset Of         | Third-Party Services  | TPM-04   | Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).   | 10                       |       |
| SA-9-IS.3    | External Information System Services                 | The AE must notify CMS at least 45 days prior to transmitting data into an external information system environment.   | Functional     | Subset Of         | Third-Party Services  | TPM-04   | Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).   | 10                       |       |
| SA-9(1)      | Risk Assessments/Organizational Approvals            | The organization conducts an organizational assessment of risk prior to the acquisition or outsourcing of information services.   | Functional     | Subset Of         | 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-9(1)-IS.1 | Risk Assessments/Organizational Approvals            | The organization documents all existing outsourced information services and conducts a risk assessment of future outsourced information services.   | Functional     | Subset Of         | 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-9(2)      | Identification of Functions/Ports/Protocols/Services | The organization requires providers of defined external information system services (defined in the applicable security plan) to identify the functions, ports, protocols, and other services required for the use of such services.  | Functional     | Subset Of         | External Connectivity Requirements/ Identification of Ports, Protocols & Services | TPM-04.2 | Mechanisms exist to require External Service Providers (ESPs) to identify and document the business need for ports, protocols and other services it requires to operate its Technology Assets, Applications and/or Services (TAAS).  | 10                       |       |

| FDE #        | FDE Name   | Focal Document Element (FDE) Description  | STRM Rationale | STRM Relationship | SCF Control  | SCF #    | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes                     |
|--------------|--|---|----------------|-------------------|--|----------|--|--------------------------|---------------------------|
| SA-9(5)      | Processing, Storage, and Service Location                  | The outsourcing of information system services outside the continental U.S. must be authorized by the CIO of CMS. Depending on the outcome of the risk assessment, the organization may need to restrict the location of information systems that receive, process, store, or transmit PII to areas within United States territories, embassies, or military installations.   | 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 include statutory, regulatory and contractual obligations.  | 5                        |                           |
| SA-9(5)      | Processing, Storage, and Service Location                  | The outsourcing of information system services outside the continental U.S. must be authorized by the CIO of CMS. Depending on the outcome of the risk assessment, the organization may need to restrict the location of information systems that receive, process, store, or transmit PII to areas within United States territories, embassies, or military installations.   | Functional     | Intersects With   | Third-Party Processing, Storage and Service Locations                  | TPM-04.4 | Mechanisms exist to restrict the location of information processing/storage based on business requirements.  | 5                        |                           |
| SA-9(5)      | Processing, Storage, and Service Location                  | The outsourcing of information system services outside the continental U.S. must be authorized by the CIO of CMS. Depending on the outcome of the risk assessment, the organization may need to restrict the location of information systems that receive, process, store, or transmit PII to areas within United States territories, embassies, or military installations.   | 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-10        | Developer Configuration Management                         | The organization requires the information system developers/integrators to:   | Functional     | Subset Of         | 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.a      | Developer Configuration Management                         | Perform configuration management during system, component, or service development, implementation, and operation;   | Functional     | Subset Of         | 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.b      | Developer Configuration Management                         | Document, manage, and control the integrity of changes to the information system;   | Functional     | Subset Of         | 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.c      | Developer Configuration Management                         | Implement only organization-approved changes to the system, component, or service;  | Functional     | Subset Of         | 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.d      | Developer Configuration Management                         | Document approved changes to the information system; and  | Functional     | Subset Of         | 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.e      | Developer Configuration Management                         | Track security flaws and flaw resolution within the system, component, or service and report findings to defined personnel or roles.  | Functional     | Subset Of         | 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-11        | Developer Security Testing and Evaluation                  | The organization requires the developer of the information system, system component, or information system service to:  | Functional     | Subset Of         | Security, Compliance & Resilience Testing Throughout Development       | TDA-09   | Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and(3) Document the results. | 10                       |                           |
| SA-11.a      | Developer Security Testing and Evaluation                  | Create and implement a security assessment plan in accordance with, but not limited to, current organization procedures;  | Functional     | Subset Of         | Security, Compliance & Resilience Testing Throughout Development       | TDA-09   | Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and(3) Document the results. | 10                       |                           |
| SA-11.b      | Developer Security Testing and Evaluation                  | Perform unit, integration, system, regression testing/evaluation in accordance with organizational defined system development life cycle;   | Functional     | Subset Of         | Security, Compliance & Resilience Testing Throughout Development       | TDA-09   | Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and(3) Document the results. | 10                       |                           |
| SA-11.c      | Developer Security Testing and Evaluation                  | Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;   | Functional     | Subset Of         | Security, Compliance & Resilience Testing Throughout Development       | TDA-09   | Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and(3) Document the results. | 10                       |                           |
| SA-11.d      | Developer Security Testing and Evaluation                  | Implement a verifiable flaw remediation process; and  | Functional     | Subset Of         | Security, Compliance & Resilience Testing Throughout Development       | TDA-09   | Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and(3) Document the results. | 10                       |                           |
| SA-11.e      | Developer Security Testing and Evaluation                  | Correct flaws identified during security testing/evaluation.  | Functional     | Subset Of         | Security, Compliance & Resilience Testing Throughout Development       | TDA-09   | Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and(3) Document the results. | 10                       |                           |
| SA-11.H.1    | Developer Security Testing and Evaluation                  | If the security control assessment results are used in support of the security authorization process for the information system, ensure that no security relevant modifications of the information systems have been made subsequent to the assessment and after selective verification of the results.   | Functional     | Subset Of         | Security, Compliance & Resilience Testing Throughout Development       | TDA-09   | Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and(3) Document the results. | 10                       |                           |
| SA-11.H.2    | Developer Security Testing and Evaluation                  | Use hypothetical data when executing test scripts or in a test environment that is configured to comply with the security controls as if it is a production environment.  | Functional     | Subset Of         | Secure Baseline Configurations   | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.  | 10                       |                           |
| SA-11.H.3    | Developer Security Testing and Evaluation                  | All systems supporting development and pre-production testing are connected to an isolated network separated from production systems. Network traffic into and out of the development and pre-production testing environment is only permitted to facilitate system testing, and is restricted by source and destination access control lists as well as ports and protocols. | Functional     | Subset Of         | Security, Compliance & Resilience Testing Throughout Development       | TDA-09   | Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and(3) Document the results. | 10                       |                           |
| SA-11(I)     | Static Code Analysis                                       | The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.  | Functional     | Subset Of         | 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(I)-H.1 | Static Code Analysis                                       | The organization submits a code analysis report as part of the authorization package and update the report in any reauthorization actions.  | Functional     | Subset Of         | 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(I)-H.2 | Static Code Analysis                                       | The organization documents in the Continuous Monitoring Plan how newly developed code for the information system is reviewed.   | Functional     | Subset Of         | 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-22        | Unsupported System Components                              | The organization:   | Functional     | Subset Of         | Unsupported Technology Assets, Applications and/or Services (TAAS)     | TDA-17   | Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by:(1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and(2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.                           | 10                       |                           |
| SA-22        | Unsupported System Components                              | The organization:   | Functional     | Intersects With   | Alternate Sources for Continued Support                                | TDA-17.1 | Mechanisms exist to provide in-house support or contract external providers for support with unsupported Technology Assets, Applications and/or Services (TAAS).   | 5                        |                           |
| SA-22.a      | Unsupported System Components                              | Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and  | Functional     | Subset Of         | Unsupported Technology Assets, Applications and/or Services (TAAS)     | TDA-17   | Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by:(1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and(2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.                           | 10                       |                           |
| SA-22.b      | Unsupported System Components                              | Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.  | Functional     | Subset Of         | Unsupported Technology Assets, Applications and/or Services (TAAS)     | TDA-17   | Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by:(1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and(2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.                           | 10                       |                           |
| 1.16         | System and Communications Protection (SC)                  | N/A   | Functional     | No Relationship   | N/A  | N/A      | N/A  | 0                        | No applicable SCF control |
| SC-1         | System and Communications Protection Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days.   | Functional     | Intersects With   | Publishing Security, Compliance & Resilience Documentation             | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, complete and resilient capabilities.  | 5                        |                           |
| SC-1         | System and Communications Protection Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days.   | Functional     | Subset Of         | Network Security Controls (NSC)  | NET-01   | Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).   | 10                       |                           |
| SC-1         | System and Communications Protection Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days.   | Functional     | Subset Of         | Secure Engineering Principles  | SEA-01   | Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).   | 10                       |                           |
| SC-1         | System and Communications Protection Policy and Procedures | The organization develops, documents, and disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days.   | Functional     | Intersects With   | Periodic Review & Update of Security, Compliance & Resilience Program  | GOV-03   | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRIP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.   | 5                        |                           |

| FDE #       | FDE Name   | Focal Document Element (FDE) Description  | STRM Rationale | STRM Relationship | SCF Control  | SCF #    | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes |
|-------------|--|---|----------------|-------------------|--|----------|--|--------------------------|-------|
| SC-1.a      | System and Communications Protection Policy and Procedures | A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  | Functional     | Subset Of         | Publishing Security, Compliance & Resilience Documentation | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.   | 10                       |       |
| SC-1.b      | System and Communications Protection Policy and Procedures | Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.  | Functional     | Subset Of         | Standardized Operating Procedures (SOP)                    | OPS-01.1 | Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.  | 10                       |       |
| SC-2        | Application Partitioning                                   | The information system separates user functionality, including user interface services (e.g., web services), from information system management (e.g., database management systems) functionality.  | Functional     | Subset Of         | Application Partitioning                                   | SEA-03.2 | Mechanisms exist to separate user functionality from system management functionality.  | 10                       |       |
| SC-4        | Information in Shared Resources                            | The information system prevents unauthorized and unintended information transfer via shared system resources.   | Functional     | Subset Of         | Information in Shared Resources                            | SEA-05   | Mechanisms exist to prevent unauthorized and unintended information transfer via shared system resources.  | 10                       |       |
| SC-4-5.1    | Information in Shared Resources                            | Ensure that users of shared system resources cannot intentionally or unintentionally access information remnants, including encrypted representations of information, produced by the actions of a prior user or system process acting on behalf of a prior user.   | Functional     | Subset Of         | Information in Shared Resources                            | SEA-05   | Mechanisms exist to prevent unauthorized and unintended information transfer via shared system resources.  | 10                       |       |
| SC-4-5.2    | Information in Shared Resources                            | Ensure that system resources shared between two (2) or more users are released back to the information system, and are protected from accidental or purposeful disclosure.  | Functional     | Subset Of         | Information in Shared Resources                            | SEA-05   | Mechanisms exist to prevent unauthorized and unintended information transfer via shared system resources.  | 10                       |       |
| SC-5        | Denial of Service Protection                               | The information system protects against or limits the effects of the types of denial of service attacks defined on the following websites by employing security safeguards (defined in the applicable security plan):   | 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-5        | Denial of Service Protection                               | The information system protects against or limits the effects of the types of denial of service attacks defined on the following websites by employing security safeguards (defined in the applicable security plan):   | 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-5        | Denial of Service Protection                               | The information system protects against or limits the effects of the types of denial of service attacks defined on the following websites by employing security safeguards (defined in the applicable security plan):   | 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-5        | Denial of Service Protection                               | The information system protects against or limits the effects of the types of denial of service attacks defined on the following websites by employing security safeguards (defined in the applicable security plan):   | Functional     | Subset Of         | Denial of Service (DoS) Protection                         | NET-02.1 | Automated mechanisms exist to protect against or limit the effects of denial of service attacks.   | 10                       |       |
| SC-5.a      | Denial of Service Protection                               | SANS Organization: <a href="http://www.sans.org/dosstep">www.sans.org/dosstep</a> ;   | Functional     | Subset Of         | Denial of Service (DoS) Protection                         | NET-02.1 | Automated mechanisms exist to protect against or limit the effects of denial of service attacks.   | 10                       |       |
| SC-5.b      | Denial of Service Protection                               | SANS Organization's Roadmap to Defeating DDOS: <a href="http://www.sans.org/dosstep">www.sans.org/dosstep</a> ; and   | Functional     | Subset Of         | Denial of Service (DoS) Protection                         | NET-02.1 | Automated mechanisms exist to protect against or limit the effects of denial of service attacks.   | 10                       |       |
| SC-5.c      | Denial of Service Protection                               | NIST National Vulnerability Database: <a href="http://nvd.nist.gov/vuln.cfm">http://nvd.nist.gov/vuln.cfm</a> .   | Functional     | Subset Of         | Denial of Service (DoS) Protection                         | NET-02.1 | Automated mechanisms exist to protect against or limit the effects of denial of service attacks.   | 10                       |       |
| SC-5-15     | Denial of Service Protection                               | The organization defines a list of types of denial of service attacks (including but not limited to denial of service and softwarelogic attacks) or provides a reference to source for current list.  | Functional     | Subset Of         | Denial of Service (DoS) Protection                         | NET-02.1 | Automated mechanisms exist to protect against or limit the effects of denial of service attacks.   | 10                       |       |
| SC-6        | Resource Availability                                      | The information system protects the availability of resources by allocating resources by priority and/or quota.   | 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-7        | Boundary Protection  | The information system:   | Functional     | Subset Of         | Boundary Protection  | NET-03   | Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.   | 10                       |       |
| SC-7.a      | Boundary Protection  | Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;   | Functional     | Subset Of         | Boundary Protection  | NET-03   | Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.   | 10                       |       |
| SC-7.b      | Boundary Protection  | Implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks; and  | Functional     | Subset Of         | Boundary Protection  | NET-03   | Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.   | 10                       |       |
| SC-7.c      | Boundary Protection  | Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.   | Functional     | Subset Of         | Boundary Protection  | NET-03   | Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.   | 10                       |       |
| SC-7-5.1    | Boundary Protection  | Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.  | Functional     | Subset Of         | Boundary Protection  | NET-03   | Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.   | 10                       |       |
| SC-7-5.2    | Boundary Protection  | Utilize stateful inspection/application firewall hardware and software.   | Functional     | Subset Of         | Boundary Protection  | NET-03   | Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.   | 10                       |       |
| SC-7-5.3    | Boundary Protection  | Utilize firewalls from at least two (2) different vendors at the various levels within the network to reduce the possibility of compromising the entire network.  | Functional     | Subset Of         | Boundary Protection  | NET-03   | Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.   | 10                       |       |
| SC-7(3)     | Access Points  | The organization limits the number of external network connections to the information system.   | Functional     | Subset Of         | 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-7(4)     | External Telecommunications Services                       | The organization:   | Functional     | Subset Of         | 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.   | 10                       |       |
| SC-7(4).a   | External Telecommunications Services                       | Implements a managed interface for each external telecommunication service;   | Functional     | Subset Of         | 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.   | 10                       |       |
| SC-7(4).b   | External Telecommunications Services                       | Establishes a traffic flow policy for each managed interface;   | Functional     | Subset Of         | 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.   | 10                       |       |
| SC-7(4).c   | External Telecommunications Services                       | Employs security controls as needed to protect the confidentiality and integrity of the information transmitted;  | Functional     | Subset Of         | 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.   | 10                       |       |
| SC-7(4).d   | External Telecommunications Services                       | Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;  | Functional     | Subset Of         | 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.   | 10                       |       |
| SC-7(4).e   | External Telecommunications Services                       | Reviews exceptions to the traffic flow policy within every three hundred sixty-five (365) days; and   | Functional     | Subset Of         | 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.   | 10                       |       |
| SC-7(4).f   | External Telecommunications Services                       | Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.   | Functional     | Subset Of         | 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.   | 10                       |       |
| SC-7(5)     | Deny by Default/Allow by Exception                         | The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).   | 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-7(7)     | Prevent Split Tunneling for Remote Devices                 | The information system, in conjunction with a remote device, prevents the device from establishing or remoting connections with the system and communicating via some other connection to resources in external networks.   | Functional     | Subset Of         | Split Tunneling  | CFG-03.4 | Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.  | 10                       |       |
| SC-7(8)     | Route Traffic to Authenticated Proxy Servers               | The information system routes organization-defined internal communications traffic to organization-defined external networks through authenticated proxy servers within the managed interfaces of boundary protection devices.  | Functional     | Subset Of         | Route Internal Traffic to Proxy Servers                    | NET-18.1 | Mechanisms exist to route internal communications traffic to external networks through organization-approved proxy servers at managed interfaces.  | 10                       |       |
| SC-7(8)     | Route Traffic to Authenticated Proxy Servers               | The information system routes organization-defined internal communications traffic to organization-defined external networks through authenticated proxy servers within the managed interfaces of boundary protection devices.  | 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-7(8)-5.1 | Route Traffic to Authenticated Proxy Servers               | The organization defines the internal communications traffic to be routed by the information system through authenticated proxy servers and the external networks that are the prospective destination of such traffic routing.   | Functional     | Subset Of         | Route Internal Traffic to Proxy Servers                    | NET-18.1 | Mechanisms exist to route internal communications traffic to external networks through organization-approved proxy servers at managed interfaces.  | 10                       |       |
| SC-7(12)    | Host-Based Protection                                      | The organization implements defined, host-based boundary protection mechanisms at defined information system components, including servers, workstations, and mobile devices.   | Functional     | Subset Of         | Host-Based Security Function Isolation                     | END-16.1 | Mechanisms exist to implement underlying software separation mechanisms to facilitate security function isolation.   | 10                       |       |
| SC-7(13)    | Isolation of Security Tools/Mechanisms/Support Components  | The organization defines key information security tools, mechanisms, and support components associated with system and security administration; and isolates those tools, mechanisms, and support components from other internal information system components via physically or logical separate subnets.  | 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 system.             | 5                        |       |
| SC-7(18)    | Fail Secure  | The information system fails securely in the event of an operational failure of a boundary protection device.   | Functional     | Intersects With   | Secure Engineering Principles                              | SEA-01   | Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS). | 5                        |       |
| SC-8        | Transmission Confidentiality and Integrity                 | The information system protects the confidentiality and integrity of transmitted information.   | Functional     | Intersects With   | Transmission Confidentiality                               | CRY-03   | Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.   | 5                        |       |
| SC-8        | Transmission Confidentiality and Integrity                 | The information system protects the confidentiality and integrity of transmitted information.   | Functional     | Intersects With   | Transmission Integrity                                     | CRY-04   | Cryptographic mechanisms exist to protect the integrity of data being transmitted.   | 5                        |       |
| SC-8-5.1    | Transmission Confidentiality and Integrity                 | Employ appropriate approved mechanisms (e.g., digital signatures and cryptographic hashes) to protect the integrity of data while in transit from source to the information outside of a secured network (see SC-13).   | Functional     | Intersects With   | Transmission Integrity                                     | CRY-04   | Cryptographic mechanisms exist to protect the integrity of data being transmitted.   | 5                        |       |
| SC-8(1)     | Cryptographic or Alternate Physical Protection             | The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by defined alternative physical safeguards (defined in the applicable security plan). This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a)(6). | Functional     | Intersects With   | Alternate Physical Protection                              | CRY-01.1 | Cryptographic mechanisms exist to prevent unauthorized disclosure of information as an alternative to physical safeguards.   | 5                        |       |
| SC-8(1)     | Cryptographic or Alternate Physical Protection             | The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by defined alternative physical safeguards (defined in the applicable security plan). This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a)(6). | Functional     | Intersects With   | Use of Cryptographic Controls                              | CRY-01   | Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.   | 5                        |       |
| SC-8(1)     | Cryptographic or Alternate Physical Protection             | The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by defined alternative physical safeguards (defined in the applicable security plan). This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a)(6). | Functional     | Intersects With   | Transmission Confidentiality                               | CRY-03   | Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.   | 5                        |       |
| SC-8(2)     | PrePost Transmission Handling                              | The information system maintains the confidentiality and integrity of information during preparation for transmission and during reception.   | Functional     | Intersects With   | PrePost Transmission Handling                              | CRY-01.3 | Cryptographic mechanisms exist to ensure the confidentiality and integrity of information during preparation for transmission and during reception.  | 5                        |       |
| SC-8(2)     | PrePost Transmission Handling                              | The information system maintains the confidentiality and integrity of information during preparation for transmission and during reception.   | Functional     | Intersects With   | Use of Cryptographic Controls                              | CRY-01   | Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.   | 5                        |       |
| SC-8(2)     | PrePost Transmission Handling                              | The information system maintains the confidentiality and integrity of information during preparation for transmission and during reception.   | Functional     | Intersects With   | Media Use  | DCH-10   | Mechanisms exist to restrict the use of types of digital media on systems or system components.  | 5                        |       |
| SC-10       | Network Disconnect   | The information system terminates the network connection associated with a communications session at the end of the session, or:  | Functional     | Subset Of         | 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                       |       |

| FDE #           | FDE Name  | Focal Document Element (FDE) Description   | STRM Rationale | STRM Relationship | SCF Control  | SCF #    | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes                     |
|-----------------|---|--|----------------|-------------------|--|----------|--|--------------------------|---------------------------|
| SC-10.a         | Network Disconnect  | Forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven (7) days; and<br>Forcibly disconnects inactive Virtual Private Network (VPN) connections after thirty (30) minutes or less of inactivity.   | Functional     | Subset Of         | 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.b         | Network Disconnect  | Forcibly disconnects inactive Virtual Private Network (VPN) connections after thirty (30) minutes or less of inactivity.   | Functional     | Subset Of         | Network Connection Termination   | NET-07   | Mechanisms exist to terminate network connections at the end of a session or after an organization-defined time period of inactivity.  | 10                       |                           |
| SC-12           | Cryptographic Key Establishment and Management                    | When cryptography is required and used within the information system, the organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with defined requirements (defined in, or referred to by, the applicable security plan) 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(2)        | Symmetric Keys  | The organization produces, controls, and distributes symmetric cryptographic keys using organization-defined key management technology and processes.  | Functional     | Subset Of         | 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-13           | Cryptographic Protection  | When cryptographic mechanisms are used, the information system implements encryption products that have been validated under the Cryptographic Module Validation Program (see <a href="http://csrc.nist.gov/groups/STM/cmvp/validation.html">http://csrc.nist.gov/groups/STM/cmvp/validation.html</a> ) to confirm compliance with FIPS 140-2, in accordance with applicable federal laws, directives, policies, regulations, and standards. | Functional     | Intersects With   | Encrypting Data At Rest  | CRY-05   | Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.   | 5                        |                           |
| SC-13           | Cryptographic Protection  | When cryptographic mechanisms are used, the information system implements encryption products that have been validated under the Cryptographic Module Validation Program (see <a href="http://csrc.nist.gov/groups/STM/cmvp/validation.html">http://csrc.nist.gov/groups/STM/cmvp/validation.html</a> ) to confirm compliance with FIPS 140-2, in accordance with applicable federal laws, directives, policies, regulations, and standards. | 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           | Cryptographic Protection  | When cryptographic mechanisms are used, the information system implements encryption products that have been validated under the Cryptographic Module Validation Program (see <a href="http://csrc.nist.gov/groups/STM/cmvp/validation.html">http://csrc.nist.gov/groups/STM/cmvp/validation.html</a> ) to confirm compliance with FIPS 140-2, in accordance with applicable federal laws, directives, policies, regulations, and standards. | Functional     | Intersects With   | Use of Cryptographic Controls  | CRY-01   | Mechanisms exist to facilitate the implementation of cryptographic protection controls using known public standards and trusted cryptographic technologies.  | 5                        |                           |
| SC-15           | Collaborative Computing Device                                    | The organization prohibits running collaborative computing mechanisms, unless explicitly authorized, in writing, by the organization's CIO or designated representative. If collaborative computing is authorized, the authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system used on the collaborative computing mechanisms. The information system:                                     | Functional     | Subset Of         | Collaborative Computing Devices  | END-14   | Mechanisms exist to unplug or prohibit the remote activation of collaborative computing devices with the following exceptions:(1) Networked whiteboards; (2) Video teleconference cameras; and(3) Teleconference microphones.                                | 10                       |                           |
| SC-15.a         | Collaborative Computing Device                                    | Prohibits remote activation of collaborative computing devices; and  | Functional     | Subset Of         | Collaborative Computing Devices  | END-14   | Mechanisms exist to unplug or prohibit the remote activation of collaborative computing devices with the following exceptions:(1) Networked whiteboards; (2) Video teleconference cameras; and(3) Teleconference microphones.                                | 10                       |                           |
| SC-15.b         | Collaborative Computing Device                                    | Provides an explicit indication of use to users physically present at the devices.   | Functional     | Subset Of         | Collaborative Computing Devices  | END-14   | Mechanisms exist to unplug or prohibit the remote activation of collaborative computing devices with the following exceptions:(1) Networked whiteboards; (2) Video teleconference cameras; and(3) Teleconference microphones.                                | 10                       |                           |
| SC-17           | Public Key Infrastructure Certificates                            | The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates from an approved service provider.  | Functional     | Intersects With   | Public Key Infrastructure (PKI)  | CRY-08   | Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.  | 5                        |                           |
| SC-18           | Mobile Code   | The organization:  | Functional     | Subset Of         | Mobile Code  | END-10   | Mechanisms exist to address mobile code / operating system-independent applications.   | 10                       |                           |
| SC-18.a         | Mobile Code   | Defines acceptable and unacceptable mobile code and mobile code technologies;  | Functional     | Subset Of         | Mobile Code  | END-10   | Mechanisms exist to address mobile code / operating system-independent applications.   | 10                       |                           |
| SC-18.b         | Mobile Code   | Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and  | Functional     | Subset Of         | Mobile Code  | END-10   | Mechanisms exist to address mobile code / operating system-independent applications.   | 10                       |                           |
| SC-18.c         | Mobile Code   | Authorizes, monitors, and controls the use of mobile code with in the information system.  | Functional     | Subset Of         | Mobile Code  | END-10   | Mechanisms exist to address mobile code / operating system-independent applications.   | 10                       |                           |
| SC-19           | Voice Over Internet Protocol                                      | The organization prohibits the use of Voice over Internet Protocol (VoIP) technologies, unless explicitly authorized, in writing, by the CIO or designated representative. If authorized, the organization:  | Functional     | Subset Of         | Voice Over Internet Protocol (VoIP) Security                             | AST-21   | Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.  | 10                       |                           |
| SC-19.a         | Voice Over Internet Protocol                                      | Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously; and   | Functional     | Subset Of         | Voice Over Internet Protocol (VoIP) Security                             | AST-21   | Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.  | 10                       |                           |
| SC-19.b         | Voice Over Internet Protocol                                      | Authorizes, monitors, and controls the use of VoIP with in the information system.   | Functional     | Subset Of         | Voice Over Internet Protocol (VoIP) Security                             | AST-21   | Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.  | 10                       |                           |
| SC-20           | Secure Name/Address Resolution Service                            | The information system:  | Functional     | Subset Of         | 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.   | 10                       |                           |
| SC-20.a         | Secure Name/Address Resolution Service                            | Provides 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; and  | Functional     | Subset Of         | 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.   | 10                       |                           |
| SC-20.b         | Secure Name/Address Resolution Service                            | Provides 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     | Subset Of         | 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.   | 10                       |                           |
| SC-20(5.1)      | Secure Name/Address Resolution Service                            | Recursive lookups are disabled on all publicly accessible domain name system (DNS) servers.  | Functional     | Subset Of         | 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.   | 10                       |                           |
| SC-21           | Secure Name/Address Resolution Service                            | The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.   | Functional     | Subset Of         | Secure Name / Address Resolution Service (Recursive or Caching Resolver) | NET-10.2 | Mechanisms exist to perform data origin authentication and data integrity verification on the Domain Name Service (DNS) resolution responses received from authoritative sources when requested by client systems.   | 10                       |                           |
| SC-22           | Architecture and Provisioning for Name/Address Resolution Service | The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement internal/external role separation.  | Functional     | Subset Of         | Architecture & Provisioning for Name / Address Resolution Service        | NET-10.1 | Mechanisms exist to ensure systems that collectively provide Domain Name Service (DNS) resolution service are fault-tolerant and implement internal/external role separation.  | 10                       |                           |
| SC-23           | Session Authenticity  | The information system protects the authenticity of communications sessions.   | Functional     | Subset Of         | Session Integrity  | NET-09   | Mechanisms exist to protect the authenticity and integrity of communications sessions.   | 10                       |                           |
| SC-28           | Protection of Information at Rest                                 | The information system protects the confidentiality and integrity of information at rest.  | Functional     | Intersects With   | Endpoint Protection Measures   | END-02   | Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.   | 5                        |                           |
| SC-28           | Protection of Information at Rest                                 | The information system protects the confidentiality and integrity of information at rest.  | Functional     | Subset Of         | Encrypting Data At Rest  | CRY-05   | Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.   | 10                       |                           |
| SC-28(5)        | Protection of Information at Rest                                 | Sensitive information such as PII should be encrypted while at rest. If information in the service provider environment cannot be encrypted, appropriate data isolation is a potential compensating control. All mechanisms used to encrypt data must be FIPS 140-2 compliant and operate using the FIPS 140-2 compliant module. This requirement must be included in the SLA, if applicable.  | Functional     | Subset Of         | Encrypting Data At Rest  | CRY-05   | Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.   | 10                       |                           |
| SC-32           | Information System Partitioning                                   | The organization partitions the information system into defined information system components (defined in the applicable security plan) residing in separate physical domains or environments based on defined circumstances (defined in the applicable security plan) for physical separation of components.  | Functional     | Subset Of         | System Partitioning  | SEA-03.1 | Mechanisms exist to partition systems so that partitions reside in separate physical domains or environments.  | 10                       |                           |
| SC-32(5)        | Information System Partitioning                                   | When contracting with external service providers, Personally Identifiable Information (PII), as well as software and services that receive, process, store, or transmit PII must be isolated within the service provider environment to the maximum extent possible so that other service provider customers sharing physical or virtual space cannot gain access to such data or applications.  | Functional     | Subset Of         | System Partitioning  | SEA-03.1 | Mechanisms exist to partition systems so that partitions reside in separate physical domains or environments.  | 10                       |                           |
| SC-39           | Process Isolation   | The information system maintains a separate execution domain for each executing process.   | Functional     | Subset Of         | Process Isolation  | SEA-04   | Mechanisms exist to implement a separate execution domain for each executing process.  | 10                       |                           |
| SC-ACA-1        | Electronic Mail   | Controls shall be implemented to protect sensitive information that is sent via email.   | Functional     | Subset Of         | Electronic Messaging   | NET-13   | Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.  | 10                       |                           |
| SC-ACA-1-IS.a   | Electronic Mail   | Prior to sending an email, place all sensitive information in an encrypted attachment.   | Functional     | Subset Of         | Electronic Messaging   | NET-13   | Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.  | 10                       |                           |
| SC-ACA-2        | FAX Usage   | If Personally Identifiable Information (PII) is allowed to be included with fax communications, the organization establishes policies and procedures for handling fax transmissions. The organization must follow specific precautions and Implementation Standards when performing fax transmission of PII.   | Functional     | Subset Of         | Electronic Messaging   | NET-13   | Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.  | 10                       |                           |
| SC-ACA-2.a      | FAX Usage   | Transmit PII only to an authorized recipient.  | Functional     | Subset Of         | Electronic Messaging   | NET-13   | Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.  | 10                       |                           |
| SC-ACA-2-IS.1   | FAX Usage   | When sending or receiving faxes containing PII:  | Functional     | Subset Of         | Electronic Messaging   | NET-13   | Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.  | 10                       |                           |
| SC-ACA-2-IS.1.a | FAX Usage   | Fax machines must be located in a locked room with a trusted staff member having custodial coverage over outgoing and incoming transmissions or fax machines must be located in a secured area;  | Functional     | Subset Of         | Electronic Messaging   | NET-13   | Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.  | 10                       |                           |
| SC-ACA-2-IS.1.b | FAX Usage   | Accurate broadcast lists and other preset numbers of frequent fax recipients must be maintained; and   | Functional     | Subset Of         | Electronic Messaging   | NET-13   | Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.  | 10                       |                           |
| SC-ACA-2-IS.1.c | FAX Usage   | A cover sheet must be used that explicitly provides guidance to the recipient that includes a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information.   | Functional     | Subset Of         | Electronic Messaging   | NET-13   | Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.  | 10                       |                           |
| 1.17            | System and Information Integrity (SI)                             | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A  | 0                        | No applicable SCF control |
| SI-1            | System and Information Integrity Policy and Procedures            | The organization develops, disseminates, and distributes to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:  | Functional     | Intersects With   | Periodic Review & Update of Security, Compliance & Resilience Program    | GOV-03   | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.      | 5                        |                           |
| SI-1            | System and Information Integrity Policy and Procedures            | The organization develops, disseminates, and distributes to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:  | Functional     | Subset Of         | Secure Engineering Principles  | SEA-01   | Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS). | 10                       |                           |
| SI-1            | System and Information Integrity Policy and Procedures            | The organization develops, disseminates, and distributes to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days:  | Functional     | Intersects With   | Publishing Security, Compliance & Resilience Documentation               | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.   | 5                        |                           |
| SI-1.a          | System and Information Integrity Policy and Procedures            | A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  | Functional     | Subset Of         | Publishing Security, Compliance & Resilience Documentation               | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.   | 10                       |                           |
| SI-1.b          | System and Information Integrity Policy and Procedures            | Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.  | Functional     | Subset Of         | Standardized Operating Procedures (SOP)                                  | OPS-01.1 | Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.  | 10                       |                           |
| SI-2            | Flaw Remediation  | The organization:  | Functional     | Subset Of         | Vulnerability & Patch Management Program (VPM)                           | VPM-01   | Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.   | 10                       |                           |
| SI-2            | Flaw Remediation  | The organization:  | Functional     | Intersects With   | Software & Firmware Patching   | VPM-05   | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.   | 5                        |                           |
| SI-2            | Flaw Remediation  | The organization:  | Functional     | Intersects With   | Automatic Antimalware Signature Updates                                  | END-04.1 | Automated mechanisms exist to update antimalware technologies, including signature definitions.  | 5                        |                           |
| SI-2.a          | Flaw Remediation  | Identifies, reports, and corrects information system flaws;  | Functional     | Subset Of         | Vulnerability & Patch Management Program (VPM)                           | VPM-01   | Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.   | 10                       |                           |

| FDE #     | FDE Name                                    | Focal Document Element (FDE) Description   | STRM Rationale | STRM Relationship | SCF Control  | SCF #    | Secure Controls Framework (SCF) Control Description   | Strength of Relationship | Notes |
|-----------|---|--|----------------|-------------------|--|----------|---|--------------------------|-------|
| SI-2.b    | Flaw Remediation                            | Tests software and firmware updates related to flaw remediation in a test environment for effectiveness and potential side effects before initial lation;  | Functional     | Subset Of         | Vulnerability & Patch Management Program (VPM)       | VPM-01   | Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.  | 10                       |       |
| SI-2.c    | Flaw Remediation                            | Installs security-relevant software and firmware updates on production equipment on a timeframe based on the National Vulnerability Database (NVD) Vulnerability Severity Rating of the flaw as follows:   | Functional     | Subset Of         | Vulnerability & Patch Management Program (VPM)       | VPM-01   | Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.  | 10                       |       |
| SI-2.d    | Flaw Remediation                            | Incorporates flaw remediation into the organizational configuration management process with risk-based decisions. If a security patch is not applied to a security-based system or network authorized by the organization.   | Functional     | Subset Of         | Vulnerability & Patch Management Program (VPM)       | VPM-01   | Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.  | 10                       |       |
| SI-2(1)   | Central Management Enhancement              | The organization centrally manages the flaw remediation process.   | Functional     | Intersects With   | Centralized Management of Flaw Remediation Processes | VPM-05.1 | Mechanisms exist to centrally-manage the flaw remediation process.  | 5                        |       |
| SI-2(2)   | Automated Flaw Remediation Status           | The organization employs automated mechanisms monthly to determine the state of information system components with regard to flaw remediation.   | 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-3      | Malicious Code Protection                   | The organization:  | Functional     | Intersects With   | Software & Firmware Patching                         | VPM-05   | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.  | 5                        |       |
| SI-3      | Malicious Code Protection                   | The organization:  | Functional     | Intersects With   | Vulnerability & Patch Management Program (VPM)       | VPM-01   | Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.  | 5                        |       |
| SI-3      | Malicious Code Protection                   | The organization:  | Functional     | Subset Of         | Malicious Code Protection (Anti-Malware)             | END-04   | Mechanisms exist to utilize antim malware technologies to detect and eradicate malicious code.  | 10                       |       |
| SI-3      | Malicious Code Protection                   | The organization:  | Functional     | Intersects With   | Heuristic / Nonsignature-Based Detection             | END-04.4 | Mechanisms exist to utilize heuristic / nonsignature-based antim malware detection capabilities.  | 5                        |       |
| SI-3      | Malicious Code Protection                   | The organization:  | Functional     | Intersects With   | Safeguarding Data Over Open Networks                 | NET-12   | Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.  | 5                        |       |
| SI-3      | Malicious Code Protection                   | The organization:  | Functional     | Intersects With   | Automatic Antim malware Signature Updates            | END-04.1 | Automated mechanisms exist to update antim malware technologies, including signature definitions.   | 5                        |       |
| SI-3      | Malicious Code Protection                   | The organization:  | Functional     | Intersects With   | Input Data Validation                                | TDA-18   | Mechanisms exist to check the validity of information inputs.   | 5                        |       |
| SI-3.a    | Malicious Code Protection                   | Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;   | Functional     | Subset Of         | Malicious Code Protection (Anti-Malware)             | END-04   | Mechanisms exist to utilize antim malware technologies to detect and eradicate malicious code.  | 10                       |       |
| SI-3.b    | Malicious Code Protection                   | Updates malicious code protection mechanisms whenever new releases are available in accordance with Administering Entity (AE) configuration management policy and procedures;  | Functional     | Subset Of         | Malicious Code Protection (Anti-Malware)             | END-04   | Mechanisms exist to utilize antim malware technologies to detect and eradicate malicious code.  | 10                       |       |
| SI-3.c    | Malicious Code Protection                   | Configures malicious code protection mechanisms to:  | Functional     | Subset Of         | Malicious Code Protection (Anti-Malware)             | END-04   | Mechanisms exist to utilize antim malware technologies to detect and eradicate malicious code.  | 10                       |       |
| SI-3.c.1  | Malicious Code Protection                   | Perform desktop and critical system file scans every twenty-four (24) hours, and real-time scans of files from external sources at endpoint and/or network entry/exit points, as the files are downloaded, opened, or executed in accordance with AE organizational security policy; | Functional     | Subset Of         | Malicious Code Protection (Anti-Malware)             | END-04   | Mechanisms exist to utilize antim malware technologies to detect and eradicate malicious code.  | 10                       |       |
| SI-3.c.2  | Malicious Code Protection                   | Block and quarantine malicious code and send alerts to the administrator in response to malicious code detection; and  | Functional     | Subset Of         | Malicious Code Protection (Anti-Malware)             | END-04   | Mechanisms exist to utilize antim malware technologies to detect and eradicate malicious code.  | 10                       |       |
| SI-3.d    | Malicious Code Protection                   | Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.   | Functional     | Subset Of         | Malicious Code Protection (Anti-Malware)             | END-04   | Mechanisms exist to utilize antim malware technologies to detect and eradicate malicious code.  | 10                       |       |
| SI-3(1)   | Central Management                          | The organization centrally manages malicious code protection mechanisms.   | Functional     | Intersects With   | Centralized Management of Antim malware Technologies | END-04.3 | Mechanisms exist to centrally-manage antim malware technologies.  | 5                        |       |
| SI-3(2)   | Automatic Updates                           | The information system automatically updates malicious code protection mechanisms.   | Functional     | Intersects With   | Automatic Antim malware Signature Updates            | END-04.1 | Automated mechanisms exist to update antim malware technologies, including signature definitions.   | 5                        |       |
| SI-4      | Information System Monitoring               | The organization:  | Functional     | Subset Of         | Continuous Monitoring                                | MON-01   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.   | 10                       |       |
| SI-4      | Information System Monitoring               | The organization:  | 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-4      | Information System Monitoring               | The organization:  | 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-4      | Information System Monitoring               | The organization:  | Functional     | Intersects With   | Input Data Validation                                | TDA-18   | Mechanisms exist to check the validity of information inputs.   | 5                        |       |
| SI-4.a    | Information System Monitoring               | Monitors the information system to detect:   | Functional     | Subset Of         | Continuous Monitoring                                | MON-01   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.   | 10                       |       |
| SI-4.a.1  | Information System Monitoring               | Attacks and indicators of potential attacks in accordance with the current Administering Entity (AE) organization incident handling policy and procedure; and  | Functional     | Subset Of         | Continuous Monitoring                                | MON-01   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.   | 10                       |       |
| SI-4.a.2  | Information System Monitoring               | Unauthorized local, network, and remote connections;   | Functional     | Subset Of         | Continuous Monitoring                                | MON-01   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.   | 10                       |       |
| SI-4.b    | Information System Monitoring               | Monitors events on the information system to ensure the proper functioning of internal processes and controls;   | Functional     | Subset Of         | Continuous Monitoring                                | MON-01   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.   | 10                       |       |
| SI-4.c    | Information System Monitoring               | Examines system records to confirm that the system is functioning in an optimal, resilient, and secure state;  | Functional     | Subset Of         | Continuous Monitoring                                | MON-01   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.   | 10                       |       |
| SI-4.d    | Information System Monitoring               | Identifies irregularities or anomalies that are indicators of a system malfunction or compromise, and detects information system attacks;  | Functional     | Subset Of         | Continuous Monitoring                                | MON-01   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.   | 10                       |       |
| SI-4.e    | Information System Monitoring               | Monitors for unauthorized remote connections to the information system continuously in real time, and takes appropriate action if an unauthorized connection is discovered;  | Functional     | Subset Of         | Continuous Monitoring                                | MON-01   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.   | 10                       |       |
| SI-4.f    | Information System Monitoring               | Identifies unauthorized use of the information system through defined techniques and methods (defined in the applicable security plan);  | Functional     | Subset Of         | Continuous Monitoring                                | MON-01   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.   | 10                       |       |
| SI-4.g    | Information System Monitoring               | Deploys monitoring devices;  | Functional     | Subset Of         | Continuous Monitoring                                | MON-01   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.   | 10                       |       |
| SI-4.g.1  | Information System Monitoring               | Strategically within the information system to collect organization-determined essential information;  | Functional     | Subset Of         | Continuous Monitoring                                | MON-01   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.   | 10                       |       |
| SI-4.g.2  | Information System Monitoring               | Ad hoc locations within the system to track specific types of transactions of interest to the organization;  | Functional     | Subset Of         | Continuous Monitoring                                | MON-01   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.   | 10                       |       |
| SI-4.h    | Information System Monitoring               | Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;  | Functional     | Subset Of         | Continuous Monitoring                                | MON-01   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.   | 10                       |       |
| SI-4.i    | Information System Monitoring               | Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, and other organizations based on law enforcement information or other credible sources of information;         | Functional     | Subset Of         | Continuous Monitoring                                | MON-01   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.   | 10                       |       |
| SI-4.j    | Information System Monitoring               | Obtains legal opinion with regard to information system-monitoring activities in accordance with applicable state and federal laws, directives, policies, or regulations; and  | Functional     | Subset Of         | Continuous Monitoring                                | MON-01   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.   | 10                       |       |
| SI-4.k    | Information System Monitoring               | Provides specified information system monitoring information to defined personnel or roles as needed, and at the established frequency (a) as defined in the applicable security plan;   | Functional     | Subset Of         | Continuous Monitoring                                | MON-01   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.   | 10                       |       |
| SI-4.l    | Information System Monitoring               | Install Intrusion Detection/Prevention System (IDS/IPS) devices at network perimeter points and hostbased IDS/IPS sensors on critical servers.   | Functional     | Subset Of         | Continuous Monitoring                                | MON-01   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.   | 10                       |       |
| SI-4(1)   | System-Wide Intrusion Detection System      | The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.  | Functional     | Subset Of         | 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-4(2)   | Automated Tools for Real-Time Analysis      | The organization employs automated tools to support near real-time analysis of events.   | Functional     | Subset Of         | 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-4(4)   | Inbound and Outbound Communications Traffic | The information system monitors inbound and outbound communications traffic at a defined frequency (defined in the applicable security plan) for unusual or unauthorized activities or conditions.   | Functional     | Subset Of         | 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-4(5)   | System-Generated Alerts                     | The information system sends alerts to defined personnel or roles (defined in the applicable security plan) when the following indications of compromise or potential compromise occur:  | Functional     | Subset Of         | 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 situational awareness.   | 10                       |       |
| SI-4(5).a | System-Generated Alerts                     | Presence of malicious code;  | Functional     | Subset Of         | 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 situational awareness.   | 10                       |       |
| SI-4(5).b | System-Generated Alerts                     | Unauthorized export of information;  | Functional     | Subset Of         | 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 situational awareness.   | 10                       |       |
| SI-4(5).c | System-Generated Alerts                     | Signaling to an external information system; or  | Functional     | Subset Of         | 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 situational awareness.   | 10                       |       |
| SI-4(5).d | System-Generated Alerts                     | Potential intrusions.  | Functional     | Subset Of         | 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 situational awareness.   | 10                       |       |
| SI-4(14)  | Wireless Intrusion Detection                | The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.  | Functional     | Intersects With   | Wireless Network Monitoring                          | MON-01.5 | Mechanisms exist to monitor wireless network segments for: (1) Rogue wireless devices; and (2) Anomalous and/or hostile activities.   | 5                        |       |
| SI-5      | Security Alerts, Advisories, and Directives | The organization:  | Functional     | Intersects With   | Input Data Validation                                | TDA-18   | Mechanisms exist to check the validity of information inputs.   | 5                        |       |
| SI-5      | Security Alerts, Advisories, and Directives | The organization:  | Functional     | Subset Of         | Threat Intelligence Feeds                            | THR-03   | Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls. | 10                       |       |
| SI-5      | Security Alerts, Advisories, and Directives | The organization:  | 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-5.a    | Security Alerts, Advisories, and Directives | Receives information system security alerts, advisories, and directives from defined external organizations (defined in the applicable security plan) on an ongoing basis.   | Functional     | Subset Of         | Threat Intelligence Feeds                            | THR-03   | Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls. | 10                       |       |
| SI-5.b    | Security Alerts, Advisories, and Directives | Generates internal security alerts, advisories, and directives as deemed necessary;  | Functional     | Subset Of         | Threat Intelligence Feeds                            | THR-03   | Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls. | 10                       |       |
| SI-5.c    | Security Alerts, Advisories, and Directives | Disseminates security alerts, advisories, and directives to: defined personnel or roles with system administration, monitoring, and/or security responsibilities (defined in the applicable security plan); and  | Functional     | Subset Of         | Threat Intelligence Feeds                            | THR-03   | Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls. | 10                       |       |
| SI-5.d    | Security Alerts, Advisories, and Directives | Implements security directives in accordance with established timeframes, or notifies the business owner of the degree of noncompliance.   | Functional     | Subset Of         | Threat Intelligence Feeds                            | THR-03   | Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls. | 10                       |       |
| SI-6      | Security Function Verification              | The information system:  | Functional     | Subset Of         | Control Functionality Verification                   | CHG-06   | Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.   | 10                       |       |
| SI-6.a    | Security Function Verification              | Verifies the correct operation of defined security functions (defined in the applicable security plan);  | Functional     | Subset Of         | Control Functionality Verification                   | CHG-06   | Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.   | 10                       |       |

| FDE #     | FDE Name                                      | Focal Document Element (FDE) Description   | STRM Rationale | STRM Relationship | SCF Control   | SCF #    | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes                     |
|-----------|---|--|----------------|-------------------|---|----------|--|--------------------------|---------------------------|
| SI-6.b    | Security Function Verification                | Performs this verification upon system startup and restart; upon command by the administrator with appropriate privilege, periodically on a monthly basis;   | Functional     | Subset Of         | Control Functionality Verification                                    | CHG-06   | Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.  | 10                       |                           |
| SI-6.c    | Security Function Verification                | Notifies system administration of failed security verification tests; and  | Functional     | Subset Of         | Control Functionality Verification                                    | CHG-06   | Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.  | 10                       |                           |
| SI-6.d    | Security Function Verification                | Shuts the information system down, restarts the information system, or performs some other defined alternative action(s) (defined in the applicable security plan) when anomalies are discovered.  | Functional     | Subset Of         | Control Functionality Verification                                    | CHG-06   | Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.  | 10                       |                           |
| SI-7      | Software, Firmware, and Information Integrity | The organization employs integrity verification tools to detect unauthorized changes to software and information.  | 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-7      | Software, Firmware, and Information Integrity | The organization employs integrity verification tools to detect unauthorized changes to software and information.  | Functional     | Intersects With   | Safeguarding Data Over Open Networks                                  | NET-12   | Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulatory data during transmission over open, public networks.  | 5                        |                           |
| SI-7      | Software, Firmware, and Information Integrity | The organization employs integrity verification tools to detect unauthorized changes to software and information.  | Functional     | Intersects With   | Input Data Validation   | TDA-18   | Mechanisms exist to check the validity of information inputs.  | 5                        |                           |
| SI-7(1)   | Integrity Checks                              | The organization reassesses the integrity of software and information by performing daily integrity scans of the information system.   | Functional     | Subset Of         | Integrity Checks  | END-06.1 | Mechanisms exist to validate configurations through integrity checking of software and firmware.   | 10                       |                           |
| SI-7(7)   | Integration of Detection and Response         | The organization incorporates the detection of unauthorized security-relevant changes to the organizational incident response capability of the information system (defined in the applicable security plan).  | Functional     | Subset Of         | Endpoint Detection & Response (EDR)                                   | END-06.2 | Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.   | 10                       |                           |
| SI-8      | Spam Protection                               | The organization:  | Functional     | Subset Of         | 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-8.a    | Spam Protection                               | Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and  | Functional     | Subset Of         | 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-8.b    | Spam Protection                               | Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.   | Functional     | Subset Of         | 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-8(1)   | Central Management                            | The organization centrally manages spam protection mechanisms.   | Functional     | Subset Of         | 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-8(2)   | Automatic Updates                             | The information system automatically updates spam protection mechanisms.   | Functional     | Subset Of         | 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-10     | Information Input Validation                  | The information system checks the validity of defined information inputs (defined in the applicable security plan) for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.   | Functional     | Intersects With   | Safeguarding Data Over Open Networks                                  | NET-12   | Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulatory data during transmission over open, public networks.  | 5                        |                           |
| SI-10     | Information Input Validation                  | The information system checks the validity of defined information inputs (defined in the applicable security plan) for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.   | Functional     | Intersects With   | Input Data Validation   | TDA-18   | Mechanisms exist to check the validity of information inputs.  | 5                        |                           |
| SI-11     | Error Handling                                | The information system:  | Functional     | Subset Of         | 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.a   | Error Handling                                | Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and   | Functional     | Subset Of         | 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.b   | Error Handling                                | Reveals error messages only to defined personnel or roles (defined in the applicable security plan).   | Functional     | Subset Of         | Error Handling  | TDA-19   | Mechanisms exist to handle error conditions by:(1) Identifying potentially security-relevant error conditions;(2) Generating error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited; and(3) Revealing error messages only to authorized personnel.  | 10                       |                           |
| SI-12     | Information Handling and Retention            | The organization handles and retains information within the information system and information output from the system in accordance with applicable state and federal laws, directives, policies, regulations, standards, and operational requirements.                                | Functional     | Subset Of         | Data Protection   | DCH-01   | Mechanisms exist to facilitate the implementation of data protection controls.   | 10                       |                           |
| SI-12     | Information Handling and Retention            | The organization handles and retains information within the information system and information output from the system in accordance with applicable state and federal laws, directives, policies, regulations, standards, and operational requirements.                                | Functional     | Intersects With   | Media & Data Retention  | DCH-18   | Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.   | 5                        |                           |
| SI-12     | Information Handling and Retention            | The organization handles and retains information within the information system and information output from the system in accordance with applicable state and federal laws, directives, policies, regulations, standards, and operational requirements.                                | Functional     | Intersects With   | Personal Data (PD) Retention & Disposal                               | PR-05    | Mechanisms exist to:(1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purposes identified in the notice or as required by law;(2) Dispose of, destroy, erase, and/or anonymize 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-12.5.1 | Information Handling and Retention            | Retain output, including, but not limited to audit records, system reports, business and financial reports, and business records, from the information system for ten (10) years or in accordance with Administering Entry organizational requirements, whichever is more restrictive. | 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-16     | Memory Protection                             | The information system implements security safeguards to protect its memory from unauthorized code execution.  | Functional     | Subset Of         | Memory Protection   | SEA-10   | Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.   | 10                       |                           |
| 1.18      | Program Management (PM)                       | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control |
| PM-1      | Information Security Program Plan             | The organization:  | Functional     | Subset Of         | Security, Compliance & Resilience Program (SCRP)                      | GOV-01   | Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.  | 10                       |                           |
| PM-1      | Information Security Program Plan             | The organization:  | Functional     | Intersects With   | Periodic Review & Update of Security, Compliance & Resilience Program | GOV-03   | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.  | 5                        |                           |
| PM-1      | Information Security Program Plan             | The organization:  | Functional     | Intersects With   | Publishing Security, Compliance & Resilience Documentation            | GOV-02   | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.   | 5                        |                           |
| PM-1.a    | Information Security Program Plan             | Develops and disseminates an organization-wide information security program plan that:   | Functional     | Subset Of         | Security, Compliance & Resilience Program (SCRP)                      | GOV-01   | Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.  | 10                       |                           |
| PM-1.a.1  | Information Security Program Plan             | Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;  | Functional     | Subset Of         | Security, Compliance & Resilience Program (SCRP)                      | GOV-01   | Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.  | 10                       |                           |
| PM-1.a.2  | Information Security Program Plan             | Includes the identification and assignment of roles, responsible titles, management commitment, coordination among organizational entities, and compliance;  | Functional     | Subset Of         | Security, Compliance & Resilience Program (SCRP)                      | GOV-01   | Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.  | 10                       |                           |
| PM-1.a.3  | Information Security Program Plan             | Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, and cyber-physical); and  | Functional     | Subset Of         | Security, Compliance & Resilience Program (SCRP)                      | GOV-01   | Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.  | 10                       |                           |
| PM-1.a.4  | Information Security Program Plan             | Is approved by a senior official with responsibility and accountability for the risk incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;                             | Functional     | Subset Of         | Security, Compliance & Resilience Program (SCRP)                      | GOV-01   | Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.  | 10                       |                           |
| PM-1.b    | Information Security Program Plan             | Reviews the organization-wide information security program plan within every three hundred sixty-five (365) days;  | Functional     | Subset Of         | Security, Compliance & Resilience Program (SCRP)                      | GOV-01   | Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.  | 10                       |                           |
| PM-1.c    | Information Security Program Plan             | Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and   | Functional     | Subset Of         | Security, Compliance & Resilience Program (SCRP)                      | GOV-01   | Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.  | 10                       |                           |
| PM-1.d    | Information Security Program Plan             | Protects the information security program plan from unauthorized disclosure and modification.  | Functional     | Subset Of         | Security, Compliance & Resilience Program (SCRP)                      | GOV-01   | Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.  | 10                       |                           |
| PM-2      | Senior Information Security Officer           | The organization appoints a senior information security officer with the responsibility and resources to coordinate, develop, implement, and maintain an organization-wide information security program.   | Functional     | Intersects With   | Assigned Security, Compliance & Resilience Responsibilities           | GOV-04   | Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).  | 5                        |                           |
| PM-3      | Information Security Resources                | The organization:  | Functional     | Subset Of         | Security, Compliance & Resilience Resource Management                 | PRM-02   | Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.  | 10                       |                           |
| PM-3.a    | Information Security Resources                | Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;   | Functional     | Subset Of         | Security, Compliance & Resilience Resource Management                 | PRM-02   | Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.  | 10                       |                           |
| PM-3.b    | Information Security Resources                | Employs a business case to record the resources required; and  | Functional     | Subset Of         | Security, Compliance & Resilience Resource Management                 | PRM-02   | Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.  | 10                       |                           |
| PM-3.c    | Information Security Resources                | Ensures that information security resources are available for expenditure as planned.  | Functional     | Subset Of         | Security, Compliance & Resilience Resource Management                 | PRM-02   | Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.  | 10                       |                           |
| PM-4      | Plan of Action and Milestones Process         | The organization:  | Functional     | Intersects With   | Vulnerability Remediation Process                                     | VPM-02   | Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.   | 5                        |                           |
| PM-4      | Plan of Action and Milestones Process         | The organization:  | Functional     | Subset Of         | Capabilities Deficiency Tracking                                      | IAO-05   | Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency(ies);(4) Risk associated with the deficiency(ies);(5) Source deficiency identification;(6) Temporary compensative controls, if applicable.      | 10                       |                           |
| PM-4.a    | Plan of Action and Milestones Process         | Implements a process to ensure that plans of action and milestones (POA&M) for the security program and associated organizational information systems:   | Functional     | Subset Of         | Capabilities Deficiency Tracking                                      | IAO-05   | Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency(ies);(4) Risk associated with the deficiency(ies);(5) Source deficiency identification;(6) Temporary compensative controls, if applicable.      | 10                       |                           |
| PM-4.a.1  | Plan of Action and Milestones Process         | Are developed and maintained;  | Functional     | Subset Of         | Capabilities Deficiency Tracking                                      | IAO-05   | Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency(ies);(4) Risk associated with the deficiency(ies);(5) Source deficiency identification;(6) Temporary compensative controls, if applicable.      | 10                       |                           |
| PM-4.a.2  | Plan of Action and Milestones Process         | Document the remedial information security actions to adequately respond to risks to organizational operations and assets, individuals, other organizations, and the Nation;   | Functional     | Subset Of         | Capabilities Deficiency Tracking                                      | IAO-05   | Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency(ies);(4) Risk associated with the deficiency(ies);(5) Source deficiency identification;(6) Temporary compensative controls, if applicable.      | 10                       |                           |

| FDE #     | FDE Name                                       | Focal Document Element (FDE) Description   | STRM Rationale | STRM Relationship | SCF Control   | SCF #  | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes  |
|-----------|--|--|----------------|-------------------|---|--------|--|--------------------------|--|
| PM-4.a.3  | Plan of Action and Milestones Process          | Are reported in accordance with CMS reporting requirements; and  | Functional     | Subset Of         | Capabilities Deficiency Tracking                            | IAO-05 | Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POAM) or similar methodology) that formally documents, at a minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency;(4) Risk associated with the deficiency;(5) Source deficiency  | 10                       |  |
| PM-4.b    | Plan of Action and Milestones Process          | Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions   | Functional     | Subset Of         | Capabilities Deficiency Tracking                            | IAO-05 | Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POAM) or similar methodology) that formally documents, at a minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency;(4) Risk associated with the deficiency;(5) Source deficiency  | 10                       |  |
| PM-4.5.1  | Plan of Action and Milestones Process          | CMS Reporting Requirement. AEs must submit copies of their updated POAM to CMS on a quarterly basis. The POAM template (an Excel spreadsheet) used to report the status of POAM can be found at: <a href="https://cat.cms.gov/dfs/projects/cms_sca_program_security_privacy/">https://cat.cms.gov/dfs/projects/cms_sca_program_security_privacy/</a> . | Functional     | Subset Of         | Capabilities Deficiency Tracking                            | IAO-05 | Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POAM) or similar methodology) that formally documents, at a minimum:(1) Deficiency tracking number;(2) Applicable security, compliance and/or resilience control;(3) Description of the deficiency;(4) Risk associated with the deficiency;(5) Source deficiency  | 10                       |  |
| PM-5      | Information System Inventory                   | The organization develops and maintains an inventory of its information systems.   | Functional     | Intersects With   | Asset Governance  | AST-01 | Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.  | 5                        |  |
| PM-5      | Information System Inventory                   | The organization develops and maintains an inventory of its information systems.   | Functional     | Subset Of         | 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 and res 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. | 10                       |  |
| PM-6      | Information Security Measures of Performance   | The organization develops, monitors, and reports on the results of information security measures of performance.   | Functional     | Intersects With   | Assigned Security, Compliance & Resilience Responsibilities | GOV-04 | Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRIP).   | 5                        |  |
| PM-6      | Information Security Measures of Performance   | The organization develops, monitors, and reports on the results of information security measures of performance.   | Functional     | Intersects With   | Measures of Performance                                     | GOV-05 | Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRIP) measures of performance.   | 5                        |  |
| PM-7      | Enterprise Architecture                        | The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.   | Functional     | Intersects With   | Alignment With Enterprise Architecture                      | SEA-02 | Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.   | 5                        |  |
| PM-8      | Critical Infrastructure Plan                   | The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.   | Functional     | Intersects With   | Business Continuity Management System (BCMS)                | BCD-01 | Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BCDR) playbooks).   | 5                        |  |
| PM-8      | Critical Infrastructure Plan                   | The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.   | Functional     | Intersects With   | Statutory, Regulatory & Contractual Compliance              | CPL-01 | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.   | 5                        |  |
| PM-9      | Risk Management Strategy                       | The organization:  | Functional     | Subset Of         | Risk Management Program                                     | RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.   | 10                       |  |
| PM-9.a    | Risk Management Strategy                       | Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems;   | Functional     | Subset Of         | Risk Management Program                                     | RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.   | 10                       |  |
| PM-9.b    | Risk Management Strategy                       | Implements the risk management strategy consistently across the organization; and  | Functional     | Subset Of         | Risk Management Program                                     | RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.   | 10                       |  |
| PM-9.c    | Risk Management Strategy                       | Reviews and updates the risk management strategy as required to address organizational changes.  | Functional     | Subset Of         | Risk Management Program                                     | RSK-01 | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.   | 10                       |  |
| PM-10.1   | Security Authorization Process                 | The organization:  | Functional     | Subset Of         | Information Assurance (IA) Operations                       | IAO-01 | Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.  | 10                       |  |
| PM-10.1a  | Security Authorization Process                 | Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes.  | Functional     | Subset Of         | Information Assurance (IA) Operations                       | IAO-01 | Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.  | 10                       | Overlapping subpoint letters, first of series  |
| PM-10.1b  | Security Authorization Process                 | Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and   | Functional     | Subset Of         | Information Assurance (IA) Operations                       | IAO-01 | Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.  | 10                       | Overlapping subpoint letters, first of series  |
| PM-10.1c  | Security Authorization Process                 | Fully integrates the security authorization processes into an organization-wide risk management program.   | Functional     | Subset Of         | Information Assurance (IA) Operations                       | IAO-01 | Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.  | 10                       | Overlapping subpoint letters, first of series  |
| PM-10.2   | Security Authorization Process                 | The Administering Entity's Authorizing Official:   | Functional     | Subset Of         | Information Assurance (IA) Operations                       | IAO-01 | Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.  | 10                       | Overlapping subpoint letters, second of series |
| PM-10.2a  | Security Authorization Process                 | Grants/denies the Authorization To Operate (ATO) based on the evaluation of security risks;  | Functional     | Subset Of         | Information Assurance (IA) Operations                       | IAO-01 | Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.  | 10                       | Overlapping subpoint letters, second of series |
| PM-10.2b  | Security Authorization Process                 | Manages the CMS-established Authority to Connect (ATC) process;  | Functional     | Subset Of         | Information Assurance (IA) Operations                       | IAO-01 | Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.  | 10                       | Overlapping subpoint letters, second of series |
| PM-10.2c  | Security Authorization Process                 | If the organization maintains a system-to-system connection with CMS through an executed Interconnection Security Agreement with CMS, CMS grants/denies the "Authority to Connect"; and  | Functional     | Subset Of         | Information Assurance (IA) Operations                       | IAO-01 | Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.  | 10                       | Overlapping subpoint letters, second of series |
| PM-10.2d  | Security Authorization Process                 | Grants/denies the authorization to establish system-to-system connections with other external entities.  | Functional     | Subset Of         | Information Assurance (IA) Operations                       | IAO-01 | Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.  | 10                       | Overlapping subpoint letters, second of series |
| PM-11     | Mission/Business Process Definition            | The organization:  | Functional     | Subset Of         | Business Process Definition                                 | PRM-06 | Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.  | 10                       |  |
| PM-11.a   | Mission/Business Process Definition            | Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and   | Functional     | Subset Of         | Business Process Definition                                 | PRM-06 | Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.  | 10                       |  |
| PM-11.b   | Mission/Business Process Definition            | Determines information protection needs arising from the defined mission/business processes, and revises the processes, as necessary, until it defines achievable protection needs.  | Functional     | Subset Of         | Business Process Definition                                 | PRM-06 | Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.  | 10                       |  |
| PM-12     | Insider Threat Program                         | The organization implements an insider threat program that includes a cross-discipline, insider threat incident handling team.   | Functional     | Subset Of         | Insider Threat Program                                      | THR-04 | Mechanisms exist to implement an insider threat program that includes a cross-discipline insider threat incident handling team.  | 10                       |  |
| PM-13     | Information Security Workforce                 | The organization establishes an information security workforce development and improvement program.  | Functional     | Intersects With   | Defined Roles & Responsibilities                            | HRS-03 | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.   | 5                        |  |
| PM-13     | Information Security Workforce                 | The organization establishes an information security workforce development and improvement program.  | Functional     | Intersects With   | Security, Compliance & Resilience-Minded Workforce          | SAT-01 | Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.  | 5                        |  |
| PM-14     | Testing, Training, and Monitoring              | The organization:  | Functional     | Subset Of         | Personal Data (PD) Control Testing, Training & Monitoring   | PRI-08 | Mechanisms exist to conduct testing, training and monitoring activities for Personal Data (PD) controls.   | 10                       |  |
| PM-14     | Testing, Training, and Monitoring              | The organization:  | Functional     | Intersects With   | Security, Compliance & Resilience Controls Oversight        | CPL-02 | Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.   | 5                        |  |
| PM-14.a   | Testing, Training, and Monitoring              | Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems.   | Functional     | Subset Of         | Personal Data (PD) Control Testing, Training & Monitoring   | PRI-08 | Mechanisms exist to conduct testing, training and monitoring activities for Personal Data (PD) controls.   | 10                       |  |
| PM-14.a.1 | Testing, Training, and Monitoring              | Are developed and maintained;  | Functional     | Subset Of         | Personal Data (PD) Control Testing, Training & Monitoring   | PRI-08 | Mechanisms exist to conduct testing, training and monitoring activities for Personal Data (PD) controls.   | 10                       |  |
| PM-14.a.2 | Testing, Training, and Monitoring              | Continue to be executed in a timely manner; and  | Functional     | Subset Of         | Personal Data (PD) Control Testing, Training & Monitoring   | PRI-08 | Mechanisms exist to conduct testing, training and monitoring activities for Personal Data (PD) controls.   | 10                       |  |
| PM-14.b   | Testing, Training, and Monitoring              | Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.   | Functional     | Subset Of         | Personal Data (PD) Control Testing, Training & Monitoring   | PRI-08 | Mechanisms exist to conduct testing, training and monitoring activities for Personal Data (PD) controls.   | 10                       |  |
| PM-15     | Contacts with Security Groups and Associations | The organization establishes and institutionalizes contact with selected groups and associations within the security community.  | Functional     | Intersects With   | Threat Intelligence Program                                 | THR-01 | Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.  | 5                        |  |
| PM-15     | Contacts with Security Groups and Associations | The organization establishes and institutionalizes contact with selected groups and associations within the security community.  | Functional     | Subset Of         | Contacts With Groups & Associations                         | GOV-07 | Mechanisms exist to establish contact with selected groups and associations within the security, compliance and resilience communities to:(1) Facilitate ongoing cybersecurity and data protection education and training for organizational personnel;(2) Maintain currency with recommended cybersecurity and data protection practices, techniques and technologies; and(3) Share current cybersecurity and/or data protection-related information including threats, vulnerabilities and incidents.                          | 10                       |  |
| PM-15.a   | Contacts with Security Groups and Associations | To facilitate ongoing security education and training for organizational personnel;  | Functional     | Subset Of         | Contacts With Groups & Associations                         | GOV-07 | Mechanisms exist to establish contact with selected groups and associations within the security, compliance and resilience communities to:(1) Facilitate ongoing cybersecurity and data protection education and training for organizational personnel;(2) Maintain currency with recommended cybersecurity and data protection practices, techniques and technologies; and(3) Share current cybersecurity and/or data protection-related information including threats, vulnerabilities and incidents.                          | 10                       |  |
| PM-15.b   | Contacts with Security Groups and Associations | To maintain currency with recommended security practices, techniques, and technologies; and  | Functional     | Subset Of         | Contacts With Groups & Associations                         | GOV-07 | Mechanisms exist to establish contact with selected groups and associations within the security, compliance and resilience communities to:(1) Facilitate ongoing cybersecurity and data protection education and training for organizational personnel;(2) Maintain currency with recommended cybersecurity and data protection practices, techniques and technologies; and(3) Share current cybersecurity and/or data protection-related information including threats, vulnerabilities and incidents.                          | 10                       |  |
| PM-15.c   | Contacts with Security Groups and Associations | To share current security-related information including threats, vulnerabilities, and incidents.   | Functional     | Subset Of         | Contacts With Groups & Associations                         | GOV-07 | Mechanisms exist to establish contact with selected groups and associations within the security, compliance and resilience communities to:(1) Facilitate ongoing cybersecurity and data protection education and training for organizational personnel;(2) Maintain currency with recommended cybersecurity and data protection practices, techniques and technologies; and(3) Share current cybersecurity and/or data protection-related information including threats, vulnerabilities and incidents.                          | 10                       |  |
| PM-16     | Threat Awareness Program                       | The organization implements a threat awareness program that includes a cross-organization information-sharing capability.  | Functional     | Intersects With   | Threat Intelligence Program                                 | THR-01 | Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.  | 5                        |  |

| FDE #    | FDE Name   | Focal Document Element (FDE) Description  | STRM Rationale | STRM Relationship | SCF Control   | SCF #    | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes                     |
|----------|--|---|----------------|-------------------|---|----------|--|--------------------------|---------------------------|
| 2        | Privacy Controls Detail and Control Implementation Description | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control |
| 2.1      | Authority and Purpose (AP)                                     | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control |
| AP-1     | Authority to Collect   | The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of Personally Identifiable Information (PII), either generally or in support of a specific program or information system need.   | Functional     | Intersects With   | Authority To Collect, Process, Store & Share Personal Data (PD) | PRI-04.1 | Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD), either generally or in support of a specific business process.  | 5                        |                           |
| AP-2     | Purpose Specification  | The organization describes the purpose(s) for which PII is collected, used, maintained, and shared in privacy notices and data sharing agreements.  | Functional     | Intersects With   | Purpose Specification   | PRI-02.1 | Mechanisms exist to ensure data privacy notices identify the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared.   | 5                        |                           |
| 2.2      | Accountability, Audit, and Risk Management (AR)                | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control |
| AR-1     | Governance and Privacy Program                                 | The organization:   | Functional     | Subset Of         | Data Privacy Program  | PRI-01   | Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.  | 10                       |                           |
| AR-1.a   | Governance and Privacy Program                                 | Appoints a designated privacy official accountable for developing, implementing, and maintaining an AE governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems;   | Functional     | Intersects With   | Chief Privacy Officer (CPO)                                     | PRI-01.1 | Mechanisms exist to appoint a Chief Privacy Officer (CPO) or similar role, with the authority, mission, accountability and resources to coordinate, develop and implement applicable data privacy requirements and manage data privacy risks through the organization-wide data privacy program.           | 5                        |                           |
| AR-1.b   | Governance and Privacy Program                                 | Monitors federal (and state as applicable) privacy laws and policy for changes that affect the privacy program;   | Functional     | Subset Of         | Data Privacy Program  | PRI-01   | Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.  | 10                       |                           |
| AR-1.c   | Governance and Privacy Program                                 | Allocates appropriate budget and staffing resources to implement and operate the privacy program;   | Functional     | Subset Of         | Data Privacy Program  | PRI-01   | Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.  | 10                       |                           |
| AR-1.d   | Governance and Privacy Program                                 | Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;  | Functional     | Subset Of         | Data Privacy Program  | PRI-01   | Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.  | 10                       |                           |
| AR-1.e   | Governance and Privacy Program                                 | Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and  | Functional     | Subset Of         | Data Privacy Program  | PRI-01   | Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.  | 10                       |                           |
| AR-1.f   | Governance and Privacy Program                                 | Updates the privacy plan, policies, and procedures, as required to address changing requirements, at least biennially.  | Functional     | Subset Of         | Data Privacy Program  | PRI-01   | Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.  | 10                       |                           |
| AR-2     | Privacy Impact and Risk Assessment                             | The organization:   | Functional     | Subset Of         | Data Protection Impact Assessment (DPIA)                        | RSK-10   | Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.   | 10                       |                           |
| AR-2.a   | Privacy Impact and Risk Assessment                             | Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, storage, sharing, transmitting, use, and disposal of PII; and   | Functional     | Subset Of         | Data Protection Impact Assessment (DPIA)                        | RSK-10   | Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.   | 10                       |                           |
| AR-2.b   | Privacy Impact and Risk Assessment                             | Conducts privacy impact assessments for information systems, programs, and other AE activities that pose a risk to the privacy of PII.  | Functional     | Subset Of         | Data Protection Impact Assessment (DPIA)                        | RSK-10   | Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.   | 10                       |                           |
| AR-3     | Privacy Requirements for Contractors and Service Providers     | The organization:   | Functional     | Subset Of         | Data Privacy Requirements for Contractors & Service Providers   | PRI-07.1 | Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.   | 10                       |                           |
| AR-3.a   | Privacy Requirements for Contractors and Service Providers     | Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and   | Functional     | Subset Of         | Data Privacy Requirements for Contractors & Service Providers   | PRI-07.1 | Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.   | 10                       |                           |
| AR-3.b   | Privacy Requirements for Contractors and Service Providers     | Includes privacy requirements in contracts and other acquisition-related documents.   | Functional     | Subset Of         | Data Privacy Requirements for Contractors & Service Providers   | PRI-07.1 | Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.   | 10                       |                           |
| AR-4     | Privacy Monitoring and Auditing                                | The organization:   | Functional     | Subset Of         | Personal Data (PD) Control Testing, Training & Monitoring       | PRI-08   | Mechanisms exist to conduct testing, training and monitoring activities for Personal Data (PD) controls.   | 10                       |                           |
| AR-4.a   | Privacy Monitoring and Auditing                                | Monitors and audits privacy controls and internal privacy policy as required to ensure effective implementation; and  | Functional     | Subset Of         | Personal Data (PD) Control Testing, Training & Monitoring       | PRI-08   | Mechanisms exist to conduct testing, training and monitoring activities for Personal Data (PD) controls.   | 10                       |                           |
| AR-4.b   | Privacy Monitoring and Auditing                                | Complies with HHS privacy oversight monitoring and auditing policies and procedures.  | Functional     | Subset Of         | Personal Data (PD) Control Testing, Training & Monitoring       | PRI-08   | Mechanisms exist to conduct testing, training and monitoring activities for Personal Data (PD) controls.   | 10                       |                           |
| AR-5     | Privacy Awareness and Training                                 | The organization:   | Functional     | Subset Of         | Sensitive / Regulated Data Storage, Handling & Processing       | SAT-03.3 | Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.  | 10                       |                           |
| AR-5.a   | Privacy Awareness and Training                                 | Develops, implements, and updates a comprehensive AE privacy training and awareness strategy aimed at ensuring personnel understand privacy responsibilities and procedures;  | Functional     | Subset Of         | Sensitive / Regulated Data Storage, Handling & Processing       | SAT-03.3 | Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.  | 10                       |                           |
| AR-5.b   | Privacy Awareness and Training                                 | Administer basic privacy training at least annually, and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII at least annually; and  | Functional     | Subset Of         | Sensitive / Regulated Data Storage, Handling & Processing       | SAT-03.3 | Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.  | 10                       |                           |
| AR-5.c   | Privacy Awareness and Training                                 | Ensure that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements at least annually.   | Functional     | Subset Of         | Sensitive / Regulated Data Storage, Handling & Processing       | SAT-03.3 | Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.  | 10                       |                           |
| AR-6     | Privacy Reporting  | The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance. This control does not apply to non-Federal entities. | Functional     | Intersects With   | Documenting Data Processing Activities                          | PRI-14   | Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements. | 5                        |                           |
| AR-7     | Privacy-enhanced System Design and Development                 | The organization designs information systems that support privacy with automated privacy controls.  | Functional     | Subset Of         | Secure Engineering Principles                                   | SEA-01   | Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).   | 10                       |                           |
| AR-8     | Accounting of Disclosures                                      | The organization:   | Functional     | Subset Of         | Accounting of Disclosures                                       | PRI-14.1 | Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by (1) The organization; and/or (2) Relevant third-parties that their PD was shared with.   | 10                       |                           |
| AR-8.a   | Accounting of Disclosures                                      | Keeps an accurate accounting of disclosures of information held in each system of records under its control, including:   | Functional     | Subset Of         | Accounting of Disclosures                                       | PRI-14.1 | Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by (1) The organization; and/or (2) Relevant third-parties that their PD was shared with.   | 10                       |                           |
| AR-8.a.1 | Accounting of Disclosures                                      | Date, nature, and purpose of each disclosure of a record; and   | Functional     | Subset Of         | Accounting of Disclosures                                       | PRI-14.1 | Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by (1) The organization; and/or (2) Relevant third-parties that their PD was shared with.   | 10                       |                           |
| AR-8.a.2 | Accounting of Disclosures                                      | Name and address of the person or agency to which the disclosure was made.  | Functional     | Subset Of         | Accounting of Disclosures                                       | PRI-14.1 | Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by (1) The organization; and/or (2) Relevant third-parties that their PD was shared with.   | 10                       |                           |
| AR-8.b   | Accounting of Disclosures                                      | Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and   | Functional     | Subset Of         | Accounting of Disclosures                                       | PRI-14.1 | Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by (1) The organization; and/or (2) Relevant third-parties that their PD was shared with.   | 10                       |                           |
| AR-8.c   | Accounting of Disclosures                                      | Makes the accounting of disclosures available to the person named in the record upon request.   | Functional     | Subset Of         | Accounting of Disclosures                                       | PRI-14.1 | Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by (1) The organization; and/or (2) Relevant third-parties that their PD was shared with.   | 10                       |                           |
| 2.3      | Data Quality and Integrity (DI)                                | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control |
| DI-1     | Data Quality   | The organization:   | Functional     | Subset Of         | Data Quality Operations   | DCH-22   | Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.  | 10                       |                           |
| DI-1.a   | Data Quality   | Confirms to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information;  | Functional     | Subset Of         | Data Quality Operations   | DCH-22   | Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.  | 10                       |                           |
| DI-1.b   | Data Quality   | Collects PII directly from the individual to the greatest extent practicable;   | Functional     | Subset Of         | Data Quality Operations   | DCH-22   | Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.  | 10                       |                           |
| DI-1.c   | Data Quality   | Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems as directed by the HHS Data Integrity Board; and  | Functional     | Subset Of         | Data Quality Operations   | DCH-22   | Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.  | 10                       |                           |
| DI-1.d   | Data Quality   | Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.   | Functional     | Subset Of         | Data Quality Operations   | DCH-22   | Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.  | 10                       |                           |
| DI-1(1)  | Validate PII   | The organization requests the individual or the individual's authorized representative validate PII during the collection process.  | Functional     | Intersects With   | Validate Collected Personal Data (PD)                           | PRI-04.5 | Mechanisms exist to ensure that the data subject, or authorized representative, validate Personal Data (PD) during the collection process.   | 5                        |                           |
| DI-1(2)  | Re-validate PII  | The organization requests the individual or the individual's authorized representative revalidate that PII collected is still accurate.   | Functional     | Intersects With   | Re-Validate Collected Personal Data (PD)                        | PRI-04.6 | Mechanisms exist to ensure that the data subject, or authorized representative, re-validate that Personal Data (PD) acquired during the collection process is still accurate.  | 5                        |                           |
| DI-2     | Data Integrity and Data Integrity Board                        | The organization:   | Functional     | Subset Of         | Personal Data (PD) Accuracy & Integrity                         | PRI-05.2 | Mechanisms exist to ensure the accuracy and relevance of Personal Data (PD) throughout the information lifecycle by (1) Keeping PD up-to-date; and (2) Remediating identified inaccuracies, as necessary.  | 10                       |                           |
| DI-2.a   | Data Integrity and Data Integrity Board                        | Document processes and procedures to ensure the integrity of PII through existing security controls; and  | Functional     | Subset Of         | Personal Data (PD) Accuracy & Integrity                         | PRI-05.2 | Mechanisms exist to ensure the accuracy and relevance of Personal Data (PD) throughout the information lifecycle by (1) Keeping PD up-to-date; and (2) Remediating identified inaccuracies, as necessary.  | 10                       |                           |
| DI-2.b   | Data Integrity and Data Integrity Board                        | Establishes a Data Integrity Board when appropriate to oversee organizational CMAs and to ensure those agreements comply with the computer matching provisions of the Privacy Act.  | Functional     | Subset Of         | Personal Data (PD) Accuracy & Integrity                         | PRI-05.2 | Mechanisms exist to ensure the accuracy and relevance of Personal Data (PD) throughout the information lifecycle by (1) Keeping PD up-to-date; and (2) Remediating identified inaccuracies, as necessary.  | 10                       |                           |
| DI-2(1)  | Publish Agreements on Website                                  | The organization publishes CMAs on its public website. Non-Federal entities are not required to implement this control.   | Functional     | Intersects With   | Computer Matching Agreements (CMA)                              | PRI-02.3 | Mechanisms exist to publish Computer Matching Agreements (CMA) on the organization's public website(s).  | 5                        |                           |
| 2.4      | Data Minimization and Retention (DM)                           | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control |

| FDE #   | FDE Name   | Focal Document Element (FDE) Description  | STRM Rationale | STRM Relationship | SCF Control   | SCF #    | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes                     |
|---------|--|---|----------------|-------------------|---|----------|--|--------------------------|---------------------------|
| DM-1    | Minimization of Personally Identifiable Information                                      | The organization:   | Functional     | Subset Of         | Internal Use of Personal Data (PD) For Testing, Training and Research | PRI-05.1 | Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.  | 10                       |                           |
| DM-1.a  | Minimization of Personally Identifiable Information                                      | Identifies the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection;   | Functional     | Subset Of         | Internal Use of Personal Data (PD) For Testing, Training and Research | PRI-05.1 | Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.  | 10                       |                           |
| DM-1.b  | Minimization of Personally Identifiable Information                                      | Limits the collection and retention of PII to the minimum elements identified, for the purposes described in the notice, and for which the individual has provided consent; and   | Functional     | Subset Of         | Internal Use of Personal Data (PD) For Testing, Training and Research | PRI-05.1 | Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.  | 10                       |                           |
| DM-1.c  | Minimization of Personally Identifiable Information                                      | Conducts an initial evaluation of PII holdings, and periodically review the holdings, within every 365 days, to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.                     | Functional     | Subset Of         | Internal Use of Personal Data (PD) For Testing, Training and Research | PRI-05.1 | Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.  | 10                       |                           |
| DM-1(1) | Minimization of PII/Locate/Remove/Redact/Anonymize PII                                   | The organization, where feasible and within the limits of technology, locates, and removes/redacts specified PII and/or uses anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure. | Functional     | Intersects With   | De-identification (Anonymization)                                     | DCH-23   | Mechanisms exist to anonymize data by removing Personal Data (PD) from datasets.   | 5                        |                           |
| DM-2    | Data Retention and Disposal  | The organization:   | Functional     | Intersects With   | Information Disposal  | DCH-21   | Mechanisms exist to securely dispose of, destroy or erase information.   | 5                        |                           |
| DM-2    | Data Retention and Disposal  | The organization:   | Functional     | Intersects With   | Personal Data (PD) Retention & Disposal                               | PRI-05   | Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purposes identified in the notice or as required by law; (2) Dispose of, destroy, erase, 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                        |                           |
| DM-2.a  | Data Retention and Disposal  | Retains each collection of PII for the minimum allowable time period necessary to fulfill the purpose(s) identified in the notice or as required by law;  | Functional     | Intersects With   | Personal Data (PD) Retention & Disposal                               | PRI-05   | Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purposes identified in the notice or as required by law; (2) Dispose of, destroy, erase, 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                        |                           |
| DM-2.b  | Data Retention and Disposal  | Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and  | Functional     | Intersects With   | Information Disposal  | DCH-21   | Mechanisms exist to securely dispose of, destroy or erase information.   | 5                        |                           |
| DM-2.c  | Data Retention and Disposal  | Uses legally compliant techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).   | Functional     | Intersects With   | Information Disposal  | DCH-21   | Mechanisms exist to securely dispose of, destroy or erase information.   | 5                        |                           |
| DM-2(1) | Data Retention and Disposal/System Configuration   | The organization configures information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under a record retention schedule.   | Functional     | Intersects With   | Documenting Data Processing Activities                                | PRI-14   | Mechanisms exist to document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.   | 5                        |                           |
| DM-3    | Minimization of PII Used in Testing, Training, and Research                              | The organization:   | Functional     | Subset Of         | Internal Use of Personal Data (PD) For Testing, Training and Research | PRI-05.1 | Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.  | 10                       |                           |
| DM-3.a  | Minimization of PII Used in Testing, Training, and Research                              | Develops policies and procedures that minimize the use of PII for testing, training, and research; and  | Functional     | Subset Of         | Internal Use of Personal Data (PD) For Testing, Training and Research | PRI-05.1 | Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.  | 10                       |                           |
| DM-3.b  | Minimization of PII Used in Testing, Training, and Research                              | Implements controls to protect PII used for testing, training, and research.  | Functional     | Subset Of         | Internal Use of Personal Data (PD) For Testing, Training and Research | PRI-05.1 | Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.  | 10                       |                           |
| DM-3(1) | Minimization of PII Used in Testing, Training, and Research/Risk Minimization Techniques | The organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training.  | Functional     | Subset Of         | Internal Use of Personal Data (PD) For Testing, Training and Research | PRI-05.1 | Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.  | 10                       |                           |
| 2.5     | Individual Participation and Redress (IP)  | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control |
| IP-1    | Consent  | The organization:   | Functional     | Subset Of         | Choice & Consent  | PRI-03   | Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.  | 10                       |                           |
| IP-1.a  | Consent  | Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintenance, and sharing of PII before its collection;  | Functional     | Subset Of         | Choice & Consent  | PRI-03   | Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.  | 10                       |                           |
| IP-1.b  | Consent  | Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, or retention of PII;  | Functional     | Subset Of         | Choice & Consent  | PRI-03   | Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.  | 10                       |                           |
| IP-1.c  | Consent  | Obtains consent, where feasible and appropriate, from individuals before any new uses or disclosures of previously collected PII; and   | Functional     | Subset Of         | Choice & Consent  | PRI-03   | Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.  | 10                       |                           |
| IP-1.d  | Consent  | Ensures individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.  | Functional     | Subset Of         | Choice & Consent  | PRI-03   | Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.  | 10                       |                           |
| IP-1(1) | Mechanism Supporting Itemized or Tiered Consent  | The organization implements mechanisms to support itemized or tiered consent for specific uses of data.   | Functional     | Subset Of         | Choice & Consent  | PRI-03   | Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.  | 10                       |                           |
| IP-2    | Individual Access  | The organization:   | Functional     | Subset Of         | Data Subject Empowerment  | PRI-06   | Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collection, receiving, processing, storing, transmitting, updated and/or sharing of their PD. | 10                       |                           |

| FDE #   | FDE Name   | Focal Document Element (FDE) Description  | STRM Rationale | STRM Relationship | SCF Control                                 | SCF #    | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes                     |
|---------|--|---|----------------|-------------------|---|----------|--|--------------------------|---------------------------|
| IP-2.a  | Individual Access                                | Provides individuals the ability to have access to their PII maintained in its system(s) of records.  | Functional     | Subset Of         | Data Subject Empowerment                    | PRI-06   | Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the categories of their PD being collected, received, processed, stored and shared;(5) Request correction to their PD due to inaccuracies;(6) Request erasure of their PD; and(7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD. | 10                       |                           |
| IP-2.b  | Individual Access                                | Publishes policies and/or regulations governing how individuals may request access to records maintained in the system of records;  | Functional     | Subset Of         | Data Subject Empowerment                    | PRI-06   | Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the categories of their PD being collected, received, processed, stored and shared;(5) Request correction to their PD due to inaccuracies;(6) Request erasure of their PD; and(7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD. | 10                       |                           |
| IP-2.c  | Individual Access                                | Publishes access procedures; and  | Functional     | Subset Of         | Data Subject Empowerment                    | PRI-06   | Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the categories of their PD being collected, received, processed, stored and shared;(5) Request correction to their PD due to inaccuracies;(6) Request erasure of their PD; and(7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.  | 10                       |                           |
| IP-2.d  | Individual Access                                | Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.  | Functional     | Subset Of         | Data Subject Empowerment                    | PRI-06   | Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the categories of their PD being collected, received, processed, stored and shared;(5) Request correction to their PD due to inaccuracies;(6) Request erasure of their PD; and(7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.  | 10                       |                           |
| IP-3    | Redress  | The organization:   | Functional     | Intersects With   | Updating & Correcting Personal Data (PD)    | DCH-22.1 | Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly re-identified.  | 5                        |                           |
| IP-3    | Redress  | The organization:   | Functional     | Intersects With   | Correcting Inaccurate Personal Data (PD)    | PRI-06.1 | Mechanisms exist to maintain a process for:(1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and(2) Disseminating corrections or amendments of PD to other authorized users of the PD.  | 5                        |                           |
| IP-3.a  | Redress  | Provide information to individuals concerning how to contact the relevant organization to have inaccurate PII maintained by that organization corrected or amended, as appropriate; and   | Functional     | Subset Of         | Data Subject Empowerment                    | PRI-06   | Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the categories of their PD being collected, received, processed, stored and shared;(5) Request correction to their PD due to inaccuracies;(6) Request erasure of their PD; and(7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD. | 10                       |                           |
| IP-3.b  | Redress  | Establish a process for disseminating corrections or amendments of the PII, if the inaccurate PII was maintained solely by the organization, to other authorized users of the PII, such as external information sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended. | Functional     | Intersects With   | Correcting Inaccurate Personal Data (PD)    | PRI-06.1 | Mechanisms exist to maintain a process for:(1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and(2) Disseminating corrections or amendments of PD to other authorized users of the PD.  | 5                        |                           |
| IP-4    | Complaint Management                             | The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.   | Functional     | Intersects With   | User Feedback Management                    | PRI-06.4 | Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.   | 5                        |                           |
| IP-4    | Complaint Management                             | The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.   | Functional     | Intersects With   | Service Delivery (Business Process Support) | OPS-03   | Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.   | 5                        |                           |
| IP-4(1) | Complaint Management/Response Times              | The organization responds to complaints, concerns, and questions from individuals within an (organization-defined) time period.   | Functional     | Intersects With   | User Feedback Management                    | PRI-06.4 | Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.   | 5                        |                           |
| IP-4(1) | Complaint Management/Response Times              | The organization responds to complaints, concerns, and questions from individuals within an (organization-defined) time period.   | Functional     | Intersects With   | Service Delivery (Business Process Support) | OPS-03   | Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.   | 5                        |                           |
| 2.6     | Security (SE)                                    | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control |
| SE-1    | Inventory of Personally Identifiable Information | The organization:   | Functional     | Subset Of         | Inventory of Personal Data (PD)             | PRI-05.5 | Mechanisms exist to establish and maintain a current inventory of all Technology Assets, Applications and/or Services (TAAS) that collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD).   | 10                       |                           |
| SE-1.a  | Inventory of Personally Identifiable Information | Establishes, maintains, and updates within every 365 days, an inventory of all programs and systems used for collecting, creating, using, disclosing, maintaini ng, or sharing PII; and   | Functional     | Subset Of         | Inventory of Personal Data (PD)             | PRI-05.5 | Mechanisms exist to establish and maintain a current inventory of all Technology Assets, Applications and/or Services (TAAS) that collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD).   | 10                       |                           |
| SE-1.b  | Inventory of Personally Identifiable Information | Provides each update of the PII inventory to the organization's designated privacy official or information security official to support the establishment of information security requirements for all new or modified information systems containing PII.  | Functional     | Subset Of         | Inventory of Personal Data (PD)             | PRI-05.5 | Mechanisms exist to establish and maintain a current inventory of all Technology Assets, Applications and/or Services (TAAS) that collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD).   | 10                       |                           |
| SE-2    | Privacy Incident Response                        | The organization:   | Functional     | Subset Of         | 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                       |                           |
| SE-2.a  | Privacy Incident Response                        | Develops and implements a Privacy Incident Response Plan;   | Functional     | Subset Of         | 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                       |                           |
| SE-2.b  | Privacy Incident Response                        | Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan; and   | Functional     | Subset Of         | 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                       |                           |
| SE-2.c  | Privacy Incident Response                        | Follows current CMS Incident Reporting requirements for reporting incidents to oversight organizations as defined in the incident handling documents available at: <a href="https://cmt.cms.gov/sf/projects/cms_aca_program_security_privacy">https://cmt.cms.gov/sf/projects/cms_aca_program_security_privacy</a> .                                      | Functional     | Subset Of         | 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                       |                           |
| 2.7     | Transparency (TR) Table                          | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control |

| FDE #    | FDE Name       | Focal Document Element (FDE) Description  | STRM Rationale | STRM Relationship | SCF Control         | SCF #  | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes |
|----------|----------------|---|----------------|-------------------|---------------------|--------|--|--------------------------|-------|
| TR-1     | Privacy Notice | The organization:   | Functional     | Subset Of         | Data Privacy Notice | PRI-02 | Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements. | 10                       |       |
| TR-1.a   | Privacy Notice | Provides effective notice to the public and to individuals regarding:   | Functional     | Subset Of         | Data Privacy Notice | PRI-02 | Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements. | 10                       |       |
| TR-1.a.1 | Privacy Notice | its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII;                               | Functional     | Subset Of         | Data Privacy Notice | PRI-02 | Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements. | 10                       |       |
| TR-1.a.2 | Privacy Notice | Authority for collecting PII;   | Functional     | Subset Of         | Data Privacy Notice | PRI-02 | Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements. | 10                       |       |
| TR-1.a.3 | Privacy Notice | The choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and | Functional     | Subset Of         | Data Privacy Notice | PRI-02 | Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements. | 10                       |       |
| TR-1.a.4 | Privacy Notice | The ability to access and have PII amended or corrected if necessary.   | Functional     | Subset Of         | Data Privacy Notice | PRI-02 | Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements. | 10                       |       |
| TR-1.b   | Privacy Notice | Describes:  | Functional     | Subset Of         | Data Privacy Notice | PRI-02 | Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements. | 10                       |       |
| TR-1.b.1 | Privacy Notice | The PII the organization collects and the purpose(s) for which it collects that information;  | Functional     | Subset Of         | Data Privacy Notice | PRI-02 | Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements. | 10                       |       |
| TR-1.b.2 | Privacy Notice | How the organization uses PII internally;   | Functional     | Subset Of         | Data Privacy Notice | PRI-02 | Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements. | 10                       |       |
| TR-1.b.3 | Privacy Notice | Whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing;                          | Functional     | Subset Of         | Data Privacy Notice | PRI-02 | Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements. | 10                       |       |

| FDE #    | FDE Name   | Focal Document Element (FDE) Description   | STRM Rationale | STRM Relationship | SCF Control                                       | SCF #    | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes                     |
|----------|--|--|----------------|-------------------|---|----------|--|--------------------------|---------------------------|
| TR-1.b.4 | Privacy Notice                                       | Whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent.   | Functional     | Subset Of         | Data Privacy Notice                               | PRI-02   | Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements. | 10                       |                           |
| TR-1.b.5 | Privacy Notice                                       | How individuals may obtain access to PII; and  | Functional     | Subset Of         | Data Privacy Notice                               | PRI-02   | Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements. | 10                       |                           |
| TR-1.b.6 | Privacy Notice                                       | How the PII will be protected.   | Functional     | Subset Of         | Data Privacy Notice                               | PRI-02   | Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements. | 10                       |                           |
| TR-1.c   | Privacy Notice                                       | Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before, or as soon as practicable after the change.<br><br>Publishes SORNs in the Federal Register, subject to required oversight processes, for systems containing PII. | Functional     | Subset Of         | Data Privacy Notice                               | PRI-02   | Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements. | 10                       |                           |
| TR-1(i)  | Real-time or Layered Notice                          | The organization provides real-time and/or layered notice to individuals at the time when any PII is collected.  | Functional     | Intersects With   | Real-Time or Layered Notice                       | PRI-02.7 | Mechanisms exist to provide real-time and/or layered notice when Personal Data (PD) is collected that provides data subjects with a summary of key points or more detailed information that is specific to the organization's data privacy notice.   | 5                        |                           |
| TR-2     | System of Records Notices and Privacy Act Statements | The organization:<br>Non-Federal systems are not required to implement this control. State-based systems must adhere to state laws that may require publication of a notice similar to the federal SORN and Privacy Act Statement.   | Functional     | Intersects With   | Privacy Act Statements                            | PRI-01.2 | Mechanisms exist to provide additional formal notice to individuals from whom the information is being collected that includes:(1) Notice of the authority of organizations to collect Personal Data (PD);(2) Whether providing PD is mandatory or optional;(3) The principal purpose or purposes for which the PD is to be used;(4) The intended disclosures or routine uses of the information; and(5) The consequences of not providing all or some portion of the information requested.   | 5                        |                           |
| TR-2     | System of Records Notices and Privacy Act Statements | The organization:<br>Non-Federal systems are not required to implement this control. State-based systems must adhere to state laws that may require publication of a notice similar to the federal SORN and Privacy Act Statement.   | Functional     | Intersects With   | System of Records Notice (SORN)                   | PRI-02.4 | Mechanisms exist to draft, publish and keep System of Records Notices (SORN) updated in accordance with regulatory guidance.   | 5                        |                           |
| TR-2.a   | System of Records Notices and Privacy Act Statements | Publishes SORNs in the Federal Register, subject to required oversight processes, for systems containing PII.  | Functional     | Intersects With   | System of Records Notice (SORN)                   | PRI-02.4 | Mechanisms exist to draft, publish and keep System of Records Notices (SORN) updated in accordance with regulatory guidance.   | 5                        |                           |
| TR-2.b   | System of Records Notices and Privacy Act Statements | Keeps SORNs current; and   | Functional     | Intersects With   | System of Records Notice (SORN)                   | PRI-02.4 | Mechanisms exist to draft, publish and keep System of Records Notices (SORN) updated in accordance with regulatory guidance.   | 5                        |                           |
| TR-2.c   | System of Records Notices and Privacy Act Statements | Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.  | Functional     | Intersects With   | Privacy Act Statements                            | PRI-01.2 | Mechanisms exist to provide additional formal notice to individuals from whom the information is being collected that includes:(1) Notice of the authority of organizations to collect Personal Data (PD);(2) Whether providing PD is mandatory or optional;(3) The principal purpose or purposes for which the PD is to be used;(4) The intended disclosures or routine uses of the information; and(5) The consequences of not providing all or some portion of the information requested.   | 5                        |                           |
| TR-2(i)  | Public Website Publication                           | The organization publishes SORNs on its public website.<br>Non-Federal systems are not required to implement this control. State-based systems must adhere to state laws that may require publication of a notice similar to the federal SORN and Privacy Act Statement.                                       | Functional     | Intersects With   | System of Records Notice (SORN)                   | PRI-02.4 | Mechanisms exist to draft, publish and keep System of Records Notices (SORN) updated in accordance with regulatory guidance.   | 5                        |                           |
| TR-3     | Dissemination of Privacy Program Information         | The organization:<br><br>Ensures the public has access to information about its privacy activities and is able to communicate with its designated privacy official.  | Functional     | Subset Of         | Dissemination of Data Privacy Program Information | PRI-01.3 | Mechanisms exist to:(1) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role;(2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories;(3) Utilize publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy officer(s) regarding data privacy practices; and(4) Inform data subjects when changes are made to the privacy notice and the nature of such changes.  | 10                       |                           |
| TR-3.a   | Dissemination of Privacy Program Information         | Ensures the public has access to information about its privacy activities and is able to communicate with its designated privacy official.   | Functional     | Subset Of         | Dissemination of Data Privacy Program Information | PRI-01.3 | Mechanisms exist to:(1) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role;(2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories;(3) Utilize publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy officer(s) regarding data privacy practices; and(4) Inform data subjects when changes are made to the privacy notice and the nature of such changes.  | 10                       |                           |
| TR-3.b   | Dissemination of Privacy Program Information         | Ensures its privacy practices are publicly available through organizational websites or otherwise.   | Functional     | Subset Of         | Dissemination of Data Privacy Program Information | PRI-01.3 | Mechanisms exist to:(1) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role;(2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories;(3) Utilize publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy officer(s) regarding data privacy practices; and(4) Inform data subjects when changes are made to the privacy notice and the nature of such changes.  | 10                       |                           |
| 2.8      | Use Limitation (UL)                                  | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control |
| UL-1     | Internal Use   | The organization (each AE) uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.  | Functional     | Intersects With   | Usage Restrictions of Personal Data (PD)          | PRI-05.4 | Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.   | 5                        |                           |
| UL-2     | Information Sharing with Third Parties               | The organization:<br><br>Shares PII externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes;  | Functional     | Subset Of         | 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.  | 10                       |                           |
| UL-2.a   | Information Sharing with Third Parties               | Shares PII externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes;   | Functional     | Subset Of         | 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.  | 10                       |                           |
| UL-2.b   | Information Sharing with Third Parties               | Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements (CMA), or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used;          | Functional     | Subset Of         | 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.  | 10                       |                           |
| UL-2.c   | Information Sharing with Third Parties               | Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and  | Functional     | Subset Of         | 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.  | 10                       |                           |
| UL-2.d   | Information Sharing with Third Parties               | Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.  | Functional     | Subset Of         | 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.  | 10                       |                           |