

## NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference document: Secure Controls Framework (SCF) version 2026.1  
 https://securecontrolsframework.com/set-theory-relationship-mapping-strm/  
 STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

## Focal Document:

Focal Document URL:  
 Published STRM URL:

## NIST SP 800-171 R3

https://csrc.nist.gov/publications/800171r3/final  
 https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-171-r3.pdf

| FDE #         | FDE Name           | Focal Document Element (FDE) Description  | STRM Rationale | STRM Relationship | SCF Control                                     | SCF #    | Secure Controls Framework (SCF) Control Description  | Strength of Relationship | Notes   |
|---------------|--------------------|---|----------------|-------------------|---|----------|--|--------------------------|---|
| 03.01.01      | Account Management | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control                                     |
| 03.01.01.a    | Account Management | Define the types of system accounts allowed and prohibited.   | Functional     | Subset Of         | Identity & Access Management (IAM)              | IAC-01   | Mechanisms exist to facilitate the implementation of identification and access management controls.  | 10                       |   |
| 03.01.01.a    | Account Management | Define the types of system accounts allowed and prohibited.   | 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                        |   |
| 03.01.01.b    | Account Management | Create, enable, modify, disable, and remove system accounts in accordance with policy, procedures, prerequisites, and criteria. | 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                        |   |
| 03.01.01.b    | Account Management | Create, enable, modify, disable, and remove system accounts in accordance with policy, procedures, prerequisites, and criteria. | Functional     | Intersects With   | Management Approval For New or Changed Accounts | IAC-28.1 | Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.  | 5                        |   |
| 03.01.01.c    | Account Management | Specify:  | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control                                     |
| 03.01.01.c.01 | Account Management | Authorized users of the system.   | Functional     | Intersects With   | Position Categorization                         | HRS-02   | Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.   | 5                        |   |
| 03.01.01.c.01 | Account Management | Authorized users of the system.   | Functional     | Intersects With   | 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.           | 5                        |   |
| 03.01.01.c.01 | Account Management | Authorized users of the system.   | 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                        |   |
| 03.01.01.c.01 | Account Management | Authorized users of the system.   | Functional     | Intersects With   | Restrictions on Shared Groups /Accounts         | IAC-15.5 | Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.   | 5                        |   |
| 03.01.01.c.02 | Account Management | Group and role membership, and  | Functional     | Intersects With   | Position Categorization                         | HRS-02   | Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.   | 5                        |   |
| 03.01.01.c.02 | Account Management | Group and role membership, and  | Functional     | Intersects With   | 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.           | 5                        |   |
| 03.01.01.c.02 | Account Management | Group and role membership, and  | 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                        |   |
| 03.01.01.c.03 | Account Management | Access authorizations (i.e., privileges) for each account.  | Functional     | Intersects With   | 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.           | 5                        |   |
| 03.01.01.c.03 | Account Management | Access authorizations (i.e., privileges) for each account.  | 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                        |   |
| 03.01.01.c.03 | Account Management | Access authorizations (i.e., privileges) for each account.  | Functional     | Intersects With   | Access To Sensitive / Regulated Data            | IAC-20.1 | Mechanisms exist to limit access to sensitive/regulated data to only those individuals whose job requires such access.   | 5                        |   |
| 03.01.01.c.03 | Account Management | Access authorizations (i.e., privileges) for each account.  | 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                        |   |
| 03.01.01.d    | Account Management | Authorize access to the system based on:  | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control                                     |
| 03.01.01.d.01 | Account Management | A valid access authorization and  | Functional     | Intersects With   | Data Protection                                 | DCH-01   | Mechanisms exist to facilitate the implementation of data protection controls.   | 5                        |   |
| 03.01.01.d.01 | Account Management | A valid access authorization and  | Functional     | Intersects With   | Sensitive / Regulated Data Protection           | DCH-01.2 | Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.   | 5                        |   |
| 03.01.01.d.01 | Account Management | A valid access authorization and  | Functional     | Intersects With   | Position Categorization                         | HRS-02   | Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.   | 5                        |   |
| 03.01.01.d.01 | Account Management | A valid access authorization and  | 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                        |   |
| 03.01.01.d.01 | Account Management | A valid access authorization and  | 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                        |   |
| 03.01.01.d.01 | Account Management | A valid access authorization and  | Functional     | Intersects With   | Access To Sensitive / Regulated Data            | IAC-20.1 | Mechanisms exist to limit access to sensitive/regulated data to only those individuals whose job requires such access.   | 5                        |   |
| 03.01.01.d.01 | Account Management | A valid access authorization and  | 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                        |   |
| 03.01.01.d.02 | Account Management | Intended system usage.  | Functional     | Intersects With   | Data Protection                                 | DCH-01   | Mechanisms exist to facilitate the implementation of data protection controls.   | 5                        |   |
| 03.01.01.d.02 | Account Management | Intended system usage.  | Functional     | Intersects With   | Sensitive / Regulated Data Protection           | DCH-01.2 | Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.   | 5                        |   |
| 03.01.01.d.02 | Account Management | Intended system usage.  | Functional     | Intersects With   | Position Categorization                         | HRS-02   | Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.   | 5                        |   |
| 03.01.01.d.02 | Account Management | Intended system usage.  | 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                        |   |
| 03.01.01.d.02 | Account Management | Intended system usage.  | 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                        |   |
| 03.01.01.d.02 | Account Management | Intended system usage.  | Functional     | Intersects With   | Access To Sensitive / Regulated Data            | IAC-20.1 | Mechanisms exist to limit access to sensitive/regulated data to only those individuals whose job requires such access.   | 5                        |   |
| 03.01.01.d.02 | Account Management | Intended system usage.  | 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                        |   |
| 03.01.01.e    | Account Management | Monitor the use of system accounts.   | 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                        |   |
| 03.01.01.e    | Account Management | Monitor the use of system accounts.   | Functional     | Intersects With   | System Account Reviews                          | IAC-15.7 | Mechanisms exist to review all system accounts and disable any account that cannot be associated with a business process and owner.  | 5                        |   |
| 03.01.01.e    | Account Management | Monitor the use of system accounts.   | Functional     | Intersects With   | Anomalous Behavior                              | MON-16   | Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious actions. | 5                        |   |
| 03.01.01.f    | Account Management | Disable system accounts when:   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control                                     |
| 03.01.01.f.01 | Account Management | The accounts have expired.  | 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                        |   |
| 03.01.01.f.02 | Account Management | The accounts have been inactive for [Assignment: organization-defined time period].   | Functional     | Intersects With   | Disable Inactive Accounts                       | IAC-15.3 | Automated mechanisms exist to disable inactive accounts after an organization-defined time period.   | 8                        | ODP Value: at most 90 days                                    |
| 03.01.01.f.03 | Account Management | The accounts are no longer associated with a user or individual.  | Functional     | Intersects With   | Personnel Termination                           | HRS-09   | Mechanisms exist to govern the termination of individual employment.   | 5                        |   |
| 03.01.01.f.03 | Account Management | The accounts are no longer associated with a user or individual.  | 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                        |   |
| 03.01.01.f.04 | Account Management | The accounts are in violation of organizational policy, or  | Functional     | Intersects With   | Personnel Sanctions                             | HRS-07   | Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.   | 5                        |   |
| 03.01.01.f.04 | Account Management | The accounts are in violation of organizational policy, or  | Functional     | Intersects With   | Workplace Investigations                        | HRS-07.1 | Mechanisms exist to conduct employee misconduct investigations when there is reasonable assurance that a policy has been violated.   | 5                        |   |
| 03.01.01.f.04 | Account Management | The accounts are in violation of organizational policy, or  | 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                        |   |
| 03.01.01.f.04 | Account Management | The accounts are in violation of organizational policy, or  | Functional     | Intersects With   | Account Disabling for High Risk Individuals     | IAC-15.6 | Mechanisms exist to disable accounts immediately upon notification for users posing a significant risk to the organization.  | 5                        |   |
| 03.01.01.f.05 | Account Management | Significant risks associated with individuals are discovered.   | Functional     | Intersects With   | Personnel Sanctions                             | HRS-07   | Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.   | 5                        |   |
| 03.01.01.f.05 | Account Management | Significant risks associated with individuals are discovered.   | Functional     | Intersects With   | Workplace Investigations                        | HRS-07.1 | Mechanisms exist to conduct employee misconduct investigations when there is reasonable assurance that a policy has been violated.   | 5                        |   |
| 03.01.01.f.05 | Account Management | Significant risks associated with individuals are discovered.   | 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                        |   |
| 03.01.01.f.05 | Account Management | Significant risks associated with individuals are discovered.   | Functional     | Intersects With   | Account Disabling for High Risk Individuals     | IAC-15.6 | Mechanisms exist to disable accounts immediately upon notification for users posing a significant risk to the organization.  | 5                        |   |
| 03.01.01.g    | Account Management | Notify account managers and designated personnel or roles within:   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control                                     |
| 03.01.01.g.01 | Account Management | [Assignment: organization-defined time period] when accounts are no longer required.  | Functional     | Intersects With   | User Provisioning & De-Provisioning             | IAC-07   | Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.   | 8                        | DoD-provided ODP does not apply to this specific SCF control. |
| 03.01.01.g.01 | Account Management | [Assignment: organization-defined time period] when accounts are no longer required.  | Functional     | Intersects With   | Change of Roles & Duties                        | IAC-07.1 | Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.  | 8                        | ODP Value: 24 hours   |
| 03.01.01.g.01 | Account Management | [Assignment: organization-defined time period] when accounts are no longer required.  | Functional     | Intersects With   | Account Management                              | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.  | 8                        | ODP Value: 24 hours   |
| 03.01.01.g.02 | Account Management | [Assignment: organization-defined time period] when users are terminated or transferred.  | Functional     | Intersects With   | Human Resources Security Management             | HRS-01   | Mechanisms exist to facilitate the implementation of personnel security controls.  | 5                        | DoD-provided ODP does not apply to this specific SCF control. |
| 03.01.01.g.02 | Account Management | [Assignment: organization-defined time period] when users are terminated or transferred.  | Functional     | Intersects With   | 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.                        | 8                        | ODP Value: 24 hours   |
| 03.01.01.g.02 | Account Management | [Assignment: organization-defined time period] when users are terminated or transferred.  | Functional     | Intersects With   | Personnel Termination                           | HRS-09   | Mechanisms exist to govern the termination of individual employment.   | 8                        | ODP Value: 24 hours   |
| 03.01.01.g.02 | Account Management | [Assignment: organization-defined time period] when users are terminated or transferred.  | Functional     | Intersects With   | Automated Employment Status Notifications       | HRS-09.4 | Automated mechanisms exist to notify identity and Access Management (IAM) personnel or roles upon termination of an individual employment or contract.   | 5                        | DoD-provided ODP does not apply to this specific SCF control. |
| 03.01.01.g.02 | Account Management | [Assignment: organization-defined time period] when users are terminated or transferred.  | Functional     | Intersects With   | User Provisioning & De-Provisioning             | IAC-07   | Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.   | 8                        | DoD-provided ODP does not apply to this specific SCF control. |
| 03.01.01.g.02 | Account Management | [Assignment: organization-defined time period] when users are terminated or transferred.  | Functional     | Intersects With   | Change of Roles & Duties                        | IAC-07.1 | Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.  | 8                        | ODP Value: 24 hours   |
| 03.01.01.g.02 | Account Management | [Assignment: organization-defined time period] when users are terminated or transferred.  | 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                        | DoD-provided ODP does not apply to this specific SCF control. |
| 03.01.01.g.03 | Account Management | [Assignment: organization-defined time period] when system usage or the need-to-know changes for an individual.                 | Functional     | Intersects With   | User Provisioning & De-Provisioning             | IAC-07   | Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.   | 8                        | DoD-provided ODP does not apply to this specific SCF control. |
| 03.01.01.g.03 | Account Management | [Assignment: organization-defined time period] when system usage or the need-to-know changes for an individual.                 | Functional     | Intersects With   | Change of Roles & Duties                        | IAC-07.1 | Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.  | 8                        | ODP Value: 24 hours   |
| 03.01.01.g.03 | Account Management | [Assignment: organization-defined time period] when system usage or the need-to-know changes for an individual.                 | 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                        | DoD-provided ODP does not apply to this specific 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   |
|---------------|------------------------------|--|----------------|-------------------|---|----------|---|--------------------------|---|
| 03.01.01.g.03 | Account Management           | [Assignment: organization-defined time period] when system usage or the need to know changes for an individual.  | Functional     | Intersects With   | Periodic Review of Account Privileges                         | IAC-17   | Mechanisms exist to periodically review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.01.01.h    | Account Management           | Require that users log out of the system after [Assignment: organization-defined time period] of expected inactivity or when [Assignment: organization-defined circumstances]. | Functional     | Intersects With   | Secure Baseline Configurations                                | CFG-02   | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.01.01.h    | Account Management           | Require that users log out of the system after [Assignment: organization-defined time period] of expected inactivity or when [Assignment: organization-defined circumstances]. | Functional     | Intersects With   | Terms of Employment   | HRS-05   | Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.01.01.h    | Account Management           | Require that users log out of the system after [Assignment: organization-defined time period] of expected inactivity or when [Assignment: organization-defined circumstances]. | Functional     | Intersects With   | Technology Use Restrictions                                   | HRS-05.3 | Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.01.01.h    | Account Management           | Require that users log out of the system after [Assignment: organization-defined time period] of expected inactivity or when [Assignment: organization-defined circumstances]. | Functional     | Equal             | Session Termination   | IAC-25   | Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.  | 10                       | ODP Values: (01) - at most 24 hours (02) - the work period ends, for privileged users at a minimum  |
| 03.01.02      | Access Enforcement           | Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.  | Functional     | Intersects With   | Sensitive / Regulated Data Access Enforcement                 | CFG-08   | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to restrict access to sensitive/regulated data.  | 5                        |   |
| 03.01.02      | Access Enforcement           | Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.  | Functional     | Intersects With   | Sensitive / Regulated Data Protection                         | DCH-01.2 | Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.  | 5                        |   |
| 03.01.02      | Access Enforcement           | Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.  | Functional     | Intersects With   | Defining Access Authorizations for Sensitive / Regulated Data | DCH-01.4 | Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and/or physical access to sensitive/regulated data.  | 5                        |   |
| 03.01.02      | Access Enforcement           | Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.  | Functional     | Intersects With   | Position Categorization                                       | HRS-02   | Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling these positions.  | 5                        |   |
| 03.01.02      | Access Enforcement           | Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.  | Functional     | Intersects With   | Users With Elevated Privileges                                | HRS-02.1 | Mechanisms exist to ensure that every user accessing Technology Assets, Applications and/or Services (TAAS) that process, store and/or transmit sensitive/regulated data is cleared and regularly trained to handle the information in question.  | 5                        |   |
| 03.01.02      | Access Enforcement           | Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.  | Functional     | Intersects With   | 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.  | 5                        |   |
| 03.01.02      | Access Enforcement           | Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.  | 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                        |   |
| 03.01.02      | Access Enforcement           | Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.  | Functional     | Subset Of         | Access Enforcement  | IAC-20   | Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."  | 10                       |   |
| 03.01.02      | Access Enforcement           | Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.  | Functional     | Intersects With   | Access To Sensitive / Regulated Data                          | IAC-20.1 | Mechanisms exist to limit access to sensitive/regulated data to only those individuals whose job requires such access.  | 5                        |   |
| 03.01.03      | Information Flow Enforcement | Enforce approved authorizations for controlling the flow of CUI within the system and between connected 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.   | 3                        |   |
| 03.01.03      | Information Flow Enforcement | Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.   | Functional     | Intersects With   | Asset-Service Dependencies                                    | AST-01.1 | Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.   | 8                        |   |
| 03.01.03      | Information Flow Enforcement | Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.   | Functional     | Intersects With   | Network Diagrams & Data Flow Diagrams (DFDs)                  | AST-04   | Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.  | 8                        |   |
| 03.01.03      | Information Flow Enforcement | Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.   | Functional     | Intersects With   | Compliance-Specific Asset Identification                      | AST-04.3 | Mechanisms exist to create and maintain a current inventory of Technology Assets, Applications, Services and/or Data (TAASD) that are in scope for statutory, regulatory and/or contractual compliance obligations that provides sufficient detail to determine control applicability, based on asset scope categorization.     | 8                        |   |
| 03.01.03      | Information Flow Enforcement | Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.   | Functional     | Intersects With   | Asset Categorization  | AST-31   | Mechanisms exist to categorize Technology Assets, Applications and/or Services (TAAS).  | 8                        |   |
| 03.01.03      | Information Flow Enforcement | Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.   | Functional     | Intersects With   | Defining Access Authorizations for Sensitive / Regulated Data | DCH-01.4 | Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and/or physical access to sensitive/regulated data.  | 8                        |   |
| 03.01.03      | Information Flow Enforcement | Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.   | Functional     | Intersects With   | Media Access  | DCH-03   | Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.   | 5                        |   |
| 03.01.03      | Information Flow Enforcement | Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.   | Functional     | Intersects With   | Data Access Mapping   | DCH-14.3 | Mechanisms exist to leverage data-specific Access Control Lists (ACLs) or Interconnection Security Agreements (ISAs) to generate a logical map of the parties with whom sensitive/regulated data is shared.   | 5                        |   |
| 03.01.03      | Information Flow Enforcement | Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.   | Functional     | Subset Of         | Access Enforcement  | IAC-20   | Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."  | 10                       |   |
| 03.01.03      | Information Flow Enforcement | Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.   | Functional     | Subset Of         | Access To Sensitive / Regulated Data                          | IAC-20.1 | Mechanisms exist to limit access to sensitive/regulated data to only those individuals whose job requires such access.  | 10                       |   |
| 03.01.03      | Information Flow Enforcement | Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.   | Functional     | Intersects With   | 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.  | 5                        |   |
| 03.01.03      | Information Flow Enforcement | Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.   | 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                        |   |
| 03.01.03      | Information Flow Enforcement | Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.   | Functional     | Intersects With   | 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.   | 5                        |   |
| 03.01.04      | Separation of Duties         | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A   | 0                        | No applicable SCF control   |
| 03.01.04.a    | Separation of Duties         | Identify the duties of individuals requiring separation.   | Functional     | Intersects With   | Separation of Duties (SoD)                                    | HRS-11   | Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.  | 8                        |   |
| 03.01.04.a    | Separation of Duties         | Identify the duties of individuals requiring separation.   | Functional     | Intersects With   | Incompatible Roles  | HRS-12   | Mechanisms exist to avoid incompatible development-specific roles through limiting and reviewing developer privileges to change hardware, software and firmware components within a production/operational environment.   | 8                        |   |
| 03.01.04.b    | Separation of Duties         | Define system access authorizations to support separation of duties.   | Functional     | Intersects With   | Defining Access Authorizations for Sensitive / Regulated Data | DCH-01.4 | Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and/or physical access to sensitive/regulated data.  | 8                        |   |
| 03.01.04.b    | Separation of Duties         | Define system access authorizations to support separation of duties.   | 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                        |   |
| 03.01.04.b    | Separation of Duties         | Define system access authorizations to support separation of duties.   | Functional     | Intersects With   | Access To Sensitive / Regulated Data                          | IAC-20.1 | Mechanisms exist to limit access to sensitive/regulated data to only those individuals whose job requires such access.  | 5                        |   |
| 03.01.04.b    | Separation of Duties         | Define system access authorizations to support separation of duties.   | 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                        |   |
| 03.01.05      | Least Privilege              | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A   | 0                        | No applicable SCF control   |
| 03.01.05.a    | Least Privilege              | Allow only authorized system access for users (or processes acting on behalf of users) that is necessary to accomplish assigned organizational tasks.                          | Functional     | Subset Of         | Access Enforcement  | IAC-20   | Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."  | 10                       |   |
| 03.01.05.a    | Least Privilege              | Allow only authorized system access for users (or processes acting on behalf of users) that is necessary to accomplish assigned organizational tasks.                          | Functional     | Subset Of         | Access To Sensitive / Regulated Data                          | IAC-20.1 | Mechanisms exist to limit access to sensitive/regulated data to only those individuals whose job requires such access.  | 10                       |   |
| 03.01.05.a    | Least Privilege              | Allow only authorized system access for users (or processes acting on behalf of users) that is necessary to accomplish assigned organizational tasks.                          | Functional     | Equal             | 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                       |   |
| 03.01.05.b    | Least Privilege              | Authorize access to [Assignment: organization-defined security functions] and [Assignment: organization-defined security-relevant information].                                | Functional     | Intersects With   | 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.  | 8                        | ODP Values: (01) - at a minimum and if applicable: establishing system accounts and assigning privileges, configuring access authorizations, configuring settings for events to be audited, establishing vulnerability scanning parameters, establishing intrusion detection parameters, and managing audit information (02) - at a minimum and if applicable: threat and vulnerability information, filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, security architecture, access control lists, and audit information |
| 03.01.05.b    | Least Privilege              | Authorize access to [Assignment: organization-defined security functions] and [Assignment: organization-defined security-relevant information].                                | 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                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.01.05.b    | Least Privilege              | Authorize access to [Assignment: organization-defined security functions] and [Assignment: organization-defined security-relevant 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."  | 8                        | ODP Values: (01) - at a minimum and if applicable: establishing system accounts and assigning privileges, configuring access authorizations, configuring settings for events to be audited, establishing vulnerability scanning parameters, establishing intrusion detection parameters, and managing audit information (02) - at a minimum and if applicable: threat and vulnerability information, filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, security architecture, access control lists, and audit information |
| 03.01.05.b    | Least Privilege              | Authorize access to [Assignment: organization-defined security functions] and [Assignment: organization-defined security-relevant information].                                | Functional     | Equal             | 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                       | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.01.05.c    | Least Privilege              | Review the privileges assigned to roles or classes of users [Assignment: organization-defined frequency] to validate the need for such privileges.                             | Functional     | Intersects With   | Account Management  | IAC-15   | Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.   | 8                        | ODP Value: at least every 12 months   |
| 03.01.05.c    | Least Privilege              | Review the privileges assigned to roles or classes of users [Assignment: organization-defined frequency] to validate the need for such privileges.                             | Functional     | Intersects With   | System Account Reviews  | IAC-15.7 | Mechanisms exist to review all system accounts and disable any account that cannot be associated with a business process and owner.   | 8                        | ODP Value: at least every 12 months   |
| 03.01.05.c    | Least Privilege              | Review the privileges assigned to roles or classes of users [Assignment: organization-defined frequency] to validate the need for such privileges.                             | Functional     | Intersects With   | Periodic Review of Account Privileges                         | IAC-17   | Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.01.05.d    | Least Privilege              | Reassign or remove privileges, as necessary.   | 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                        |   |

| 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   |
|------------|--|---|----------------|-------------------|---|-----------|--|--------------------------|---|
| 03.01.05.d | Least Privilege                        | Reassign or remove privileges, as necessary.  | Functional     | Intersects With   | Periodic Review of Account Privileges                             | IAC-17    | Mechanisms exist to periodically review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.  | 5                        |   |
| 03.01.06   | Least Privilege - Privileged Accounts  | N/A   | Functional     | No Relationship   | N/A   | N/A       | N/A  | 0                        | No applicable SCF control   |
| 03.01.06.a | Least Privilege - Privileged Accounts  | Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].  | Functional     | Intersects With   | 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.   | 8                        | ODP Value: only defined and authorized personnel or administrative roles  |
| 03.01.06.a | Least Privilege - Privileged Accounts  | Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].  | Functional     | Intersects With   | Privileged Account Management (PAM)                               | IAC-16    | Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).  | 8                        | ODP Value: only defined and authorized personnel or administrative roles  |
| 03.01.06.a | Least Privilege - Privileged Accounts  | Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].  | 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                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.01.06.a | Least Privilege - Privileged Accounts  | Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].  | 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                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.01.06.a | Least Privilege - Privileged Accounts  | Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].  | Functional     | Intersects With   | Management Approval For Privileged Accounts                       | IAC-21.3  | Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles.  | 8                        | ODP Value: only defined and authorized personnel or administrative roles  |
| 03.01.06.b | Least Privilege - Privileged Accounts  | Require that users (or roles) with privileged accounts use non-privileged accounts when accessing non-security functions or non-sensitive information.  | Functional     | Intersects With   | 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.   | 5                        |   |
| 03.01.07   | Least Privilege - Privileged Functions | N/A   | Functional     | No Relationship   | N/A   | N/A       | N/A  | 0                        | No applicable SCF control   |
| 03.01.07.a | Least Privilege - Privileged Functions | Prevent non-privileged users from executing privileged functions.   | Functional     | Intersects With   | Privileged Account Management (PAM)                               | IAC-16    | Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).  | 5                        |   |
| 03.01.07.a | Least Privilege - Privileged Functions | Prevent non-privileged users from executing privileged functions.   | 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                        |   |
| 03.01.07.a | Least Privilege - Privileged Functions | Prevent non-privileged users from executing privileged functions.   | Functional     | Intersects With   | Management Approval For Privileged Accounts                       | IAC-21.3  | Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles.  | 5                        |   |
| 03.01.07.a | Least Privilege - Privileged Functions | Prevent non-privileged users from executing privileged functions.   | Functional     | Equal             | Prohibit Non-Privileged Users from Executing Privileged Functions | IAC-21.5  | Mechanisms exist to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures.  | 10                       |   |
| 03.01.07.b | Least Privilege - Privileged Functions | Log the execution of privileged functions.  | Functional     | Intersects With   | Privileged Account Identifiers                                    | IAC-09.5  | Mechanisms exist to uniquely manage privileged accounts to identify the account as a privileged user or service.   | 5                        |   |
| 03.01.07.b | Least Privilege - Privileged Functions | Log the execution of privileged functions.  | Functional     | Intersects With   | Privileged Account Management (PAM)                               | IAC-16    | Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).  | 5                        |   |
| 03.01.07.b | Least Privilege - Privileged Functions | Log the execution of privileged functions.  | Functional     | Intersects With   | Auditing Use of Privileged Functions                              | IAC-21.4  | Mechanisms exist to audit the execution of privileged functions.   | 5                        |   |
| 03.01.07.b | Least Privilege - Privileged Functions | Log the execution of privileged functions.  | Functional     | Intersects With   | Privileged User Oversight   | MON-01.15 | Mechanisms exist to implement enhanced activity monitoring for privileged users.   | 5                        |   |
| 03.01.07.b | Least Privilege - Privileged Functions | Log the execution of privileged functions.  | Functional     | Intersects With   | Privileged Functions Logging                                      | MON-03.3  | Mechanisms exist to log and review the actions of users and/or services with elevated privileges.  | 5                        |   |
| 03.01.08   | Unsuccessful Logon Attempts            | N/A   | Functional     | No Relationship   | N/A   | N/A       | N/A  | 0                        | No applicable SCF control   |
| 03.01.08.a | Unsuccessful Logon Attempts            | Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period].  | 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                       | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.01.08.a | Unsuccessful Logon Attempts            | Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period].  | Functional     | Intersects With   | 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.  | 8                        | ODP Values: (01) - at most five (5) (02) - period of five (5) minutes   |
| 03.01.08.b | Unsuccessful Logon Attempts            | Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; delay next logon prompt; notify system administrator; take other action] when the maximum number of unsuccessful attempts is exceeded.  | 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                       | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.01.08.b | Unsuccessful Logon Attempts            | Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt; notify system administrator; take other action] when the maximum number of unsuccessful attempts is exceeded. | Functional     | Intersects With   | 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.  | 8                        | ODP Value: Select one or more: lock the account or node for an at least 15-minute time period; lock the account or node until released by an administrator and notify a system administrator                                      |
| 03.01.09   | System Use Notification                | Display a system use notification message with privacy and security notices consistent with applicable CUI rules before granting 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                       |   |
| 03.01.09   | System Use Notification                | Display a system use notification message with privacy and security notices consistent with applicable CUI rules before granting access to 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                       |   |
| 03.01.09   | System Use Notification                | Display a system use notification message with privacy and security notices consistent with applicable CUI rules before granting access to the system.  | Functional     | Intersects With   | Standardized Microsoft Windows Banner                             | SEA-18.1  | Mechanisms exist to configure Microsoft Windows-based systems to display an approved logon banner before granting access to the system.  | 8                        |   |
| 03.01.09   | System Use Notification                | Display a system use notification message with privacy and security notices consistent with applicable CUI rules before granting access to the system.  | Functional     | Intersects With   | Truncated Banner  | SEA-18.2  | Mechanisms exist to utilize a truncated system use notification / logon banner on systems not capable of displaying a logon banner from a centralized directory services technology (e.g., Active Directory, Entra ID, etc.).  | 8                        |   |
| 03.01.10   | Device Lock                            | N/A   | Functional     | No Relationship   | N/A   | N/A       | N/A  | 0                        | No applicable SCF control   |
| 03.01.10.a | Device Lock                            | Prevent access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended].  | 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                       | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.01.10.a | Device Lock                            | Prevent access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended].  | 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                       | ODP Value: initiating a device lock after "at most 15 minutes" of inactivity and requiring the user to initiate a device lock before leaving the system unattended  |
| 03.01.10.b | Device Lock                            | Retain the device lock until the user reestablishes access using established identification and authentication procedures.  | 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                       |   |
| 03.01.10.b | Device Lock                            | Retain the device 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                       |   |
| 03.01.10.c | Device Lock                            | Conceal, via the device lock, information previously visible on the display with a publicly viewable image.   | 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                       |   |
| 03.01.10.c | Device Lock                            | Conceal, via the device lock, information previously visible on the display with a publicly viewable image.   | Functional     | Equal             | Pattern-Hiding Displays   | IAC-24.1  | Mechanisms exist to implement pattern-hiding displays to conceal information previously visible on the display during the session lock.  | 10                       |   |
| 03.01.11   | Session Termination                    | Terminate a user session automatically after [Assignment: organization-defined conditions or trigger events requiring session disconnect].  | 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                       | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.01.11   | Session Termination                    | Terminate a user session automatically after [Assignment: organization-defined conditions or trigger events requiring session disconnect].  | Functional     | Equal             | Session Termination   | IAC-25    | Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.   | 10                       | ODP Value: a specified duration (maximum of 24 hours) of inactivity, misbehavior (end the session due to an attempted policy violation), and maintenance (terminate sessions to prevent issues with an upgrade or service outage) |
| 03.01.12   | Remote Access                          | N/A   | Functional     | No Relationship   | N/A   | N/A       | N/A  | 0                        | No applicable SCF control   |
| 03.01.12.a | Remote Access                          | Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.  | Functional     | Intersects With   | Jump Server   | AST-27    | Mechanisms exist to conduct remote system administrative functions via a "jump box" or "jump server" that is located in a separate network zone to user workstations.  | 5                        |   |
| 03.01.12.a | Remote Access                          | Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.  | 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                        |   |
| 03.01.12.a | Remote Access                          | Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.  | Functional     | Intersects With   | Rules of Behavior   | HR5-05.1  | Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.  | 5                        |   |
| 03.01.12.a | Remote Access                          | Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.  | Functional     | Intersects With   | Technology Use Restrictions                                       | HR5-05.3  | Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.  | 5                        |   |
| 03.01.12.a | Remote Access                          | Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.  | Functional     | Intersects With   | 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.   | 5                        |   |
| 03.01.12.a | Remote Access                          | Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.  | 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                       |   |
| 03.01.12.a | Remote Access                          | Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.  | Functional     | Intersects With   | Boundary Protection   | NET-03    | Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.   | 5                        |   |
| 03.01.12.a | Remote Access                          | Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.  | Functional     | Intersects With   | Remote Access   | NET-14    | Mechanisms exist to define, control and review organization-approved, secure remote access methods.  | 5                        |   |
| 03.01.12.a | Remote Access                          | Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.  | Functional     | Intersects With   | 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).   | 5                        |   |
| 03.01.12.a | Remote Access                          | Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.  | Functional     | Intersects With   | Work From Anywhere (WFA) - Telecommuting Security                 | NET-14.5  | Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.  | 5                        |   |
| 03.01.12.a | Remote Access                          | Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.  | 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                       |   |
| 03.01.12.a | Remote Access                          | Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.  | 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                        |   |
| 03.01.12.b | Remote Access                          | Authorize each type of remote system access prior to establishing such connections.   | Functional     | Intersects With   | Remote Access   | NET-14    | Mechanisms exist to define, control and review organization-approved, secure remote access methods.  | 5                        |   |
| 03.01.12.b | Remote Access                          | Authorize each type of remote system access prior to establishing such connections.   | Functional     | Intersects With   | Automated Monitoring & Control                                    | NET-14.1  | Automated mechanisms exist to monitor and control remote access sessions.  | 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                     |
|------------|-----------------------------------|---|----------------|-------------------|---|----------|--|--------------------------|---------------------------|
| 03.01.12.b | Remote Access                     | Authorize each type of remote system access prior to establishing such connections.   | Functional     | Intersects With   | Managed Access Control Points   | NET-14.3 | Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).  | 5                        |                           |
| 03.01.12.c | Remote Access                     | Route remote access to the system through authorized and managed access control points.   | Functional     | Intersects With   | Jump Server   | AST-27   | Mechanisms exist to conduct remote system administrative functions via a "jump box" or "jump server" that is located in a separate network zone to user workstations.  | 5                        |                           |
| 03.01.12.c | Remote Access                     | Route remote access to the system through authorized and managed access control points.   | Functional     | Intersects With   | Remote Access   | NET-14   | Mechanisms exist to define, control and review organization-approved, secure remote access methods.  | 5                        |                           |
| 03.01.12.c | Remote Access                     | Route remote access to the system through authorized and managed access control points.   | Functional     | Intersects With   | Managed Access Control Points   | NET-14.3 | Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).  | 5                        |                           |
| 03.01.12.c | Remote Access                     | Route remote access to the system through authorized and managed access control points.   | Functional     | Intersects With   | Work From Anywhere (WFA) - Telecommuting Security                                       | NET-14.5 | Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAAS) for remote workers.   | 5                        |                           |
| 03.01.12.d | Remote Access                     | Authorize the remote execution of privileged commands and remote access to security-relevant information.                             | Functional     | Intersects With   | Remote Maintenance  | MNT-05   | Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.  | 5                        |                           |
| 03.01.12.d | Remote Access                     | Authorize the remote execution of privileged commands and remote access to security-relevant information.                             | Functional     | Intersects With   | Remote Access   | NET-14   | Mechanisms exist to define, control and review organization-approved, secure remote access methods.  | 5                        |                           |
| 03.01.12.d | Remote Access                     | Authorize the remote execution of privileged commands and remote access to security-relevant information.                             | Functional     | Intersects With   | 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.   | 5                        |                           |
| 03.01.13   | Withdrawn                         | Addressed by 03.13.08.  | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control |
| 03.01.14   | Withdrawn                         | Incorporated into 03.01.12.   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control |
| 03.01.15   | Withdrawn                         | Incorporated into 03.01.12.   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control |
| 03.01.16   | Wireless Access                   | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control |
| 03.01.16.a | Wireless Access                   | Establish usage restrictions, configuration requirements, and connection requirements for each type of wireless access to the 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                        |                           |
| 03.01.16.a | Wireless Access                   | Establish usage restrictions, configuration requirements, and connection requirements for each type of wireless access to the system. | Functional     | Intersects With   | Wireless Access Authentication & Encryption   | CR-07    | Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.  | 5                        |                           |
| 03.01.16.a | Wireless Access                   | Establish usage restrictions, configuration requirements, and connection requirements for each type of wireless access to the system. | 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                       |                           |
| 03.01.16.a | Wireless Access                   | Establish usage restrictions, configuration requirements, and connection requirements for each type of wireless access to the system. | Functional     | Intersects With   | Guest Networks  | NET-02.2 | Mechanisms exist to implement and manage a secure guest network.   | 5                        |                           |
| 03.01.16.a | Wireless Access                   | Establish usage restrictions, configuration requirements, and connection requirements for each type of wireless access to the system. | Functional     | Intersects With   | Wireless Networking   | NET-15   | Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.  | 5                        |                           |
| 03.01.16.a | Wireless Access                   | Establish usage restrictions, configuration requirements, and connection requirements for each type of wireless access to the system. | Functional     | Intersects With   | Authentication & Encryption   | NET-15.1 | Mechanisms exist to secure WPA1 (e.g., IEEE 802.11) and prevent unauthorized access by:<br>1) Authenticating devices trying to connect; and<br>2) Encrypting transmitted data.   | 5                        |                           |
| 03.01.16.a | Wireless Access                   | Establish usage restrictions, configuration requirements, and connection requirements for each type of wireless access to the system. | Functional     | Intersects With   | Restrict Configuration By Users   | NET-15.3 | Mechanisms exist to identify and explicitly authorize users who are allowed to independently configure wireless networking capabilities.   | 5                        |                           |
| 03.01.16.a | Wireless Access                   | Establish usage restrictions, configuration requirements, and connection requirements for each type of wireless access to the system. | 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                       |                           |
| 03.01.16.a | Wireless Access                   | Establish usage restrictions, configuration requirements, and connection requirements for each type of wireless access to the system. | 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                        |                           |
| 03.01.16.b | Wireless Access                   | Authorize each type of wireless access to the system prior to establishing such connections.  | 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                       |                           |
| 03.01.16.b | Wireless Access                   | Authorize each type of wireless access to the system prior to establishing such connections.  | Functional     | Intersects With   | Guest Networks  | NET-02.2 | Mechanisms exist to implement and manage a secure guest network.   | 5                        |                           |
| 03.01.16.b | Wireless Access                   | Authorize each type of wireless access to the system prior to establishing such connections.  | Functional     | Intersects With   | Wireless Networking   | NET-15   | Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.  | 5                        |                           |
| 03.01.16.b | Wireless Access                   | Authorize each type of wireless access to the system prior to establishing such connections.  | Functional     | Intersects With   | Authentication & Encryption   | NET-15.1 | Unauthorized access by:<br>1) Authenticating devices trying to connect; and<br>2) Encrypting transmitted data.   | 5                        |                           |
| 03.01.16.b | Wireless Access                   | Authorize each type of wireless access to the system prior to establishing such connections.  | 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                       |                           |
| 03.01.16.c | Wireless Access                   | Disable, when not intended for use, wireless networking capabilities prior to issuance and deployment.                                | Functional     | Intersects With   | Disable Wireless Networking   | NET-15.2 | Mechanisms exist to disable unnecessary wireless networking capabilities that are internally embedded within system components prior to issuance to end users.   | 5                        |                           |
| 03.01.16.c | Wireless Access                   | Disable, when not intended for use, wireless networking capabilities prior to issuance and deployment.                                | Functional     | Intersects With   | Restrict Configuration By Users   | NET-15.3 | Mechanisms exist to identify and explicitly authorize users who are allowed to independently configure wireless networking capabilities.   | 5                        |                           |
| 03.01.16.c | Wireless Access                   | Disable, when not intended for use, wireless networking capabilities prior to issuance and deployment.                                | 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                       |                           |
| 03.01.16.d | Wireless Access                   | Protect wireless access to the system using authentication and encryption.  | Functional     | Equal             | Authentication & Encryption   | NET-15.1 | Unauthorized access by:<br>1) Authenticating devices trying to connect; and<br>2) Encrypting transmitted data.   | 10                       |                           |
| 03.01.17   | Withdrawn                         | Incorporated into 03.01.16.   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control |
| 03.01.18   | Access Control for Mobile Devices | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control |
| 03.01.18.a | Access Control for Mobile Devices | Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.                             | 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                        |                           |
| 03.01.18.a | Access Control for Mobile Devices | Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.                             | Functional     | Intersects With   | Use of Personal Devices   | AST-12   | Mechanisms exist to restrict the possession and/or use of personally-owned Technology Assets, Applications and/or Services (TAAS) within organization-controlled facilities.   | 5                        |                           |
| 03.01.18.a | Access Control for Mobile Devices | Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.                             | Functional     | Intersects With   | Use of Third-Party Devices  | AST-13   | Mechanisms exist to reduce the risk associated with third-party assets that are attached to the network from harming organizational assets or exfiltrating organizational data.  | 5                        |                           |
| 03.01.18.a | Access Control for Mobile Devices | Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.                             | Functional     | Intersects With   | Usage Parameters  | AST-14   | Mechanisms exist to monitor and enforce usage parameters that limit the potential damage caused from the unauthorized or unintentional alteration of system parameters.  | 5                        |                           |
| 03.01.18.a | Access Control for Mobile Devices | Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.                             | Functional     | Intersects With   | Bring Your Own Device (BYOD) Usage  | AST-16   | Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.  | 5                        |                           |
| 03.01.18.a | Access Control for Mobile Devices | Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.                             | 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                        |                           |
| 03.01.18.a | Access Control for Mobile Devices | Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.                             | Functional     | Intersects With   | Rules of Behavior   | HRS-05.1 | Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.  | 5                        |                           |
| 03.01.18.a | Access Control for Mobile Devices | Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.                             | Functional     | Intersects With   | Technology Use Restrictions   | HRS-05.3 | Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.  | 5                        |                           |
| 03.01.18.a | Access Control for Mobile Devices | Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.                             | Functional     | Intersects With   | Use of Mobile Devices   | HRS-05.5 | Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.   | 5                        |                           |
| 03.01.18.a | Access Control for Mobile Devices | Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.                             | Functional     | Intersects With   | Access Agreements   | HRS-06   | Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.  | 5                        |                           |
| 03.01.18.a | Access Control for Mobile Devices | Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.                             | Functional     | Subset Of         | Centralized Management Of Mobile Devices  | MDM-01   | Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.  | 10                       |                           |
| 03.01.18.a | Access Control for Mobile Devices | Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.                             | Functional     | Intersects With   | 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).   | 5                        |                           |
| 03.01.18.a | Access Control for Mobile Devices | Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.                             | Functional     | Intersects With   | Personally-Owned Mobile Devices   | MDM-06   | Mechanisms exist to restrict the connection of personally-owned, mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).  | 5                        |                           |
| 03.01.18.a | Access Control for Mobile Devices | Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.                             | Functional     | Intersects With   | Organization-Owned Mobile Devices   | MDM-07   | Mechanisms exist to prohibit the installation of non-approved applications or approved applications not obtained through the organization-approved application store.  | 5                        |                           |
| 03.01.18.a | Access Control for Mobile Devices | Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.                             | Functional     | Intersects With   | Network Security Controls (NSC)   | NET-01   | Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).   | 5                        |                           |
| 03.01.18.a | Access Control for Mobile Devices | Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.                             | 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).                     | 10                       |                           |
| 03.01.18.a | Access Control for Mobile Devices | Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.                             | 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                        |                           |
| 03.01.18.b | Access Control for Mobile Devices | Authorize the connection of mobile devices to the system.   | Functional     | Subset Of         | Identity & Access Management (IAM)  | IAC-01   | Mechanisms exist to facilitate the implementation of identification and access management controls.  | 10                       |                           |
| 03.01.18.b | Access Control for Mobile Devices | Authorize the connection of mobile devices to the system.   | Functional     | Intersects With   | Identification & Authentication for Devices   | IAC-04   | Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically-based and replay resistant.  | 5                        |                           |
| 03.01.18.b | Access Control for Mobile Devices | Authorize the connection of mobile devices to the system.   | Functional     | Intersects With   | 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).   | 5                        |                           |
| 03.01.18.b | Access Control for Mobile Devices | Authorize the connection of mobile devices to the system.   | Functional     | Intersects With   | Personally-Owned Mobile Devices   | MDM-06   | Mechanisms exist to restrict the connection of personally-owned, mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).  | 5                        |                           |
| 03.01.18.b | Access Control for Mobile Devices | Authorize the connection of mobile devices to the system.   | Functional     | Intersects With   | Organization-Owned Mobile Devices   | MDM-07   | Mechanisms exist to prohibit the installation of non-approved applications or approved applications not obtained through the organization-approved application store.  | 5                        |                           |
| 03.01.18.b | Access Control for Mobile Devices | Authorize the connection of mobile devices to the system.   | Functional     | Intersects With   | Restricting Access To Authorized Technology Assets, Applications and/or Services (TAAS) | MDM-11   | Mechanisms exist to restrict the connectivity of unauthorized mobile devices from communicating with organizational Technology Assets, Applications and/or Services (TAAS).  | 5                        |                           |
| 03.01.18.c | Access Control for Mobile Devices | Implement full-device or container-based encryption to protect the confidentiality of CUI on mobile devices.                          | Functional     | Intersects With   | 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.  | 5                        |                           |
| 03.01.19   | Withdrawn                         | Incorporated into 03.01.18.   | 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   |
|---------------|-------------------------|--|----------------|-------------------|--|----------|---|--------------------------|---|
| 03.01.20      | Use of External Systems | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control   |
| 03.01.20.a    | Use of External Systems | Prohibit the use of external systems unless the systems are specifically authorized.   | Functional     | Intersects With   | Sensitive / Regulated Data Protection  | DCH-01.2 | Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.  | 5                        |   |
| 03.01.20.a    | Use of External Systems | Prohibit the use of external systems unless the systems are specifically authorized.   | Functional     | Intersects With   | 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.   | 5                        |   |
| 03.01.20.a    | Use of External Systems | Prohibit the use of external systems unless the systems are specifically authorized.   | Functional     | Intersects With   | 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:<br>(1) Verifying the implementation of required security, compliance and/or resilience controls; or<br>(2) Retaining a processing agreement with the entity hosting the external TAAS. | 5                        |   |
| 03.01.20.a    | Use of External Systems | Prohibit the use of external systems unless the systems are specifically authorized.   | 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                        |   |
| 03.01.20.a    | Use of External Systems | Prohibit the use of external systems unless the systems are specifically authorized.   | Functional     | Intersects With   | Non-Organizationally Owned Technology Assets, Applications and/or Services (TAAS)                        | DCH-13.4 | Mechanisms exist to restrict the use of non-organizationally owned Technology Assets, Applications and/or Services (TAAS) to process, store or transmit organizational information.   | 5                        |   |
| 03.01.20.a    | Use of External Systems | Prohibit the use of external systems unless the systems are specifically authorized.   | Functional     | Intersects With   | Ad-Hoc Transfers   | DCH-17   | Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.   | 5                        |   |
| 03.01.20.a    | Use of External Systems | Prohibit the use of external systems unless the systems are specifically authorized.   | Functional     | Subset Of         | Third-Party Management   | TPM-01   | Mechanisms exist to facilitate the implementation of third-party management controls.   | 10                       |   |
| 03.01.20.a    | Use of External Systems | Prohibit the use of external systems unless the systems are specifically authorized.   | Functional     | Intersects With   | Third-Party Attestation (3PA)  | TPM-05.8 | Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.   | 8                        |   |
| 03.01.20.b    | Use of External Systems | Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assignment: organization-defined security requirements]. | Functional     | Intersects With   | Sensitive / Regulated Data Protection  | DCH-01.2 | Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.  | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.01.20.b    | Use of External Systems | Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assignment: organization-defined security requirements]. | Functional     | Intersects With   | 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.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.01.20.b    | Use of External Systems | Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assignment: organization-defined security requirements]. | Functional     | Intersects With   | 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:<br>(1) Verifying the implementation of required security, compliance and/or resilience controls; or<br>(2) Retaining a processing agreement with the entity hosting the external TAAS. | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.01.20.b    | Use of External Systems | Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assignment: organization-defined security requirements]. | Functional     | Intersects With   | Protecting Sensitive / Regulated Data on External Technology Assets, Applications and/or Services (TAAS) | DCH-13.3 | Mechanisms exist to ensure that the requirements for the protection of sensitive/regulated data processed, stored or transmitted on external Technology Assets, Applications and/or Services (TAAS), are implemented in accordance with applicable statutory, regulatory and contractual obligations.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.01.20.b    | Use of External Systems | Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assignment: organization-defined security requirements]. | 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                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.01.20.b    | Use of External Systems | Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assignment: organization-defined security requirements]. | Functional     | Intersects With   | Transfer Authorizations  | DCH-14.2 | Mechanisms exist to verify that individuals or Technology Assets, Applications and/or Services (TAAS) transferring data between interconnected TAAS have the requisite authorizations (e.g., write permissions or privileges) prior to transferring said data.  | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.01.20.b    | Use of External Systems | Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assignment: organization-defined security requirements]. | Functional     | Subset Of         | Third-Party Management   | TPM-01   | Mechanisms exist to facilitate the implementation of third-party management controls.   | 10                       | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.01.20.b    | Use of External Systems | Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assignment: organization-defined security requirements]. | 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                       | ODP Value: Guidance: Organizations establish specific terms and conditions for the use of external systems in accordance with organizational security policies and procedures. At a minimum, terms and conditions address the specific types of applications that can be accessed on organizational systems from external systems and the highest security category of information that can be processed, stored, or transmitted on external systems. If the terms and conditions with the owners of the external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems. If applicable, use NIST SP 800-47 as a guide for establishing information exchanges between organizations. |
| 03.01.20.b    | Use of External Systems | Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assignment: organization-defined security requirements]. | Functional     | Intersects With   | Third-Party Attestation (3PA)  | TPM-05.8 | Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.   | 8                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.01.20.c    | Use of External Systems | Permit authorized individuals to use external systems to access the organizational system or to process, store, or transmit CUI only after:  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control   |
| 03.01.20.c.01 | Use of External Systems | Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and  | Functional     | Intersects With   | Sensitive / Regulated Data Protection  | DCH-01.2 | Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.  | 5                        |   |
| 03.01.20.c.01 | Use of External Systems | Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and  | Functional     | Intersects With   | 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.   | 5                        |   |
| 03.01.20.c.01 | Use of External Systems | Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and  | Functional     | Intersects With   | 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:<br>(1) Verifying the implementation of required security, compliance and/or resilience controls; or<br>(2) Retaining a processing agreement with the entity hosting the external TAAS. | 5                        |   |
| 03.01.20.c.01 | Use of External Systems | Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and  | Functional     | Intersects With   | Protecting Sensitive / Regulated Data on External Technology Assets, Applications and/or Services (TAAS) | DCH-13.3 | Mechanisms exist to ensure that the requirements for the protection of sensitive/regulated data processed, stored or transmitted on external Technology Assets, Applications and/or Services (TAAS), are implemented in accordance with applicable statutory, regulatory and contractual obligations.   | 5                        |   |
| 03.01.20.c.01 | Use of External Systems | Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and  | Functional     | Intersects With   | Non-Organizationally Owned Technology Assets, Applications and/or Services (TAAS)                        | DCH-13.4 | Mechanisms exist to restrict the use of non-organizationally owned Technology Assets, Applications and/or Services (TAAS) to process, store or transmit organizational information.   | 5                        |   |
| 03.01.20.c.01 | Use of External Systems | Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and  | Functional     | Subset Of         | Third-Party Management   | TPM-01   | Mechanisms exist to facilitate the implementation of third-party management controls.   | 10                       |   |
| 03.01.20.c.01 | Use of External Systems | Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and  | Functional     | Intersects With   | 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).  | 8                        |   |
| 03.01.20.c.01 | Use of External Systems | Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and  | Functional     | Intersects With   | First-Party Declaration (1PD)  | TPM-05.6 | Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to subcontractors.   | 8                        |   |
| 03.01.20.c.01 | Use of External Systems | Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and  | Functional     | Intersects With   | Third-Party Attestation (3PA)  | TPM-05.8 | Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.   | 8                        |   |
| 03.01.20.c.02 | Use of External Systems | Retaining approved system connection or processing agreements with the organizational entities hosting the external systems.   | Functional     | Intersects With   | 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.   | 5                        |   |
| 03.01.20.c.02 | Use of External Systems | Retaining approved system connection or processing agreements with the organizational entities hosting the external systems.   | Functional     | Intersects With   | 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:<br>(1) Verifying the implementation of required security, compliance and/or resilience controls; or<br>(2) Retaining a processing agreement with the entity hosting the external TAAS. | 5                        |   |
| 03.01.20.c.02 | Use of External Systems | Retaining approved system connection or processing agreements with the organizational entities hosting the external systems.   | Functional     | Intersects With   | Transfer Authorizations  | DCH-14.2 | Mechanisms exist to verify that individuals or Technology Assets, Applications and/or Services (TAAS) transferring data between interconnected TAAS have the requisite authorizations (e.g., write permissions or privileges) prior to transferring said data.  | 5                        |   |
| 03.01.20.c.02 | Use of External Systems | Retaining approved system connection or processing agreements with the organizational entities hosting the external systems.   | Functional     | Intersects With   | Data Access Mapping  | DCH-14.3 | Mechanisms exist to leverage data-specific Access Control Lists (ACL) or Interconnection Security Agreements (ISAs) to generate a logical map of the parties with whom sensitive/regulated data is shared.  | 5                        |   |
| 03.01.20.c.02 | Use of External Systems | Retaining approved system connection or processing agreements with the organizational entities hosting the external systems.   | Functional     | Intersects With   | Media & Data Retention   | DCH-18   | Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.  | 5                        |   |
| 03.01.20.c.02 | Use of External Systems | Retaining approved system connection or processing agreements with the organizational entities hosting the external systems.   | 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:<br>(1) Interface characteristics;<br>(2) Security, compliance and resilience requirements; and<br>(3) The nature of the information communicated.  | 8                        |   |
| 03.01.20.c.02 | Use of External Systems | Retaining approved system connection or processing agreements with the organizational entities hosting the external systems.   | 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                       |   |
| 03.01.20.d    | Use of External Systems | Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.  | Functional     | Intersects With   | Sensitive / Regulated Data Protection  | DCH-01.2 | Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.  | 5                        |   |
| 03.01.20.d    | Use of External Systems | Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.  | Functional     | Intersects With   | 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.   | 5                        |   |

| FDE #         | FDE Name                        | Focal Document Element (FDE) Description  | STRM Rationale | STRM Relationship | SCF Control   | SCF #    | Security Controls Framework (SCF) Control Description   | Strength of Relationship | Notes  |
|---------------|---------------------------------|---|----------------|-------------------|---|----------|---|--------------------------|--|
| 03.01.20.d    | Use of External Systems         | Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.                             | Functional     | Intersects With   | 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. | 5                        |  |
| 03.01.20.d    | Use of External Systems         | Restrict the use of organization-controlled portable storage devices by authorized individuals on external 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                        |  |
| 03.01.20.d    | Use of External Systems         | Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.                             | Functional     | Intersects With   | Non-Organizationally Owned Technology Assets, Applications and/or Services (TAAS) | DCH-13.4 | Mechanisms exist to restrict the use of non-organizationally owned Technology Assets, Applications and/or Services (TAAS) to process, store or transmit organizational information.   | 5                        |  |
| 03.01.20.d    | Use of External Systems         | Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.                             | Functional     | Subset Of         | Centralized Management Of Mobile Devices  | MDM-01   | Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.   | 10                       |  |
| 03.01.20.d    | Use of External Systems         | Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.                             | Functional     | Intersects With   | Organization-Owned Mobile Devices   | MDM-07   | Mechanisms exist to prohibit the installation of non-approved applications or approved applications not obtained through the organization-approved application store.   | 8                        |  |
| 03.01.21      | Withdrawn                       | Incorporated into 03.01.20.   | Functional     | No Relationship   | N/A   | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.01.22      | Publicly Accessible Content     | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.01.22.a    | Publicly Accessible Content     | Train authorized individuals to ensure that publicly accessible information does not contain CUI.   | Functional     | Intersects With   | Disclosure of Information   | DCH-03.1 | Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.  | 5                        |  |
| 03.01.22.a    | Publicly Accessible Content     | Train authorized individuals to ensure that publicly accessible information does not contain CUI.   | Functional     | Intersects With   | Publicly Accessible Content   | DCH-15   | Mechanisms exist to control publicly-accessible content.  | 5                        |  |
| 03.01.22.a    | Publicly Accessible Content     | Train authorized individuals to ensure that publicly accessible information does not contain CUI.   | Functional     | Intersects With   | Defined Roles & Responsibilities  | HRS-03   | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.  | 5                        |  |
| 03.01.22.a    | Publicly Accessible Content     | Train authorized individuals to ensure that publicly accessible information does not contain CUI.   | Functional     | Intersects With   | User Awareness  | HRS-03.1 | Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.  | 5                        |  |
| 03.01.22.a    | Publicly Accessible Content     | Train authorized individuals to ensure that publicly accessible information does not contain CUI.   | Functional     | Intersects With   | Roles With Special Protection Measures  | HRS-04.1 | Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.  | 5                        |  |
| 03.01.22.a    | Publicly Accessible Content     | Train authorized individuals to ensure that publicly accessible information does not contain CUI.   | Functional     | Intersects With   | Formal Indocination   | HRS-04.2 | Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access.   | 5                        |  |
| 03.01.22.a    | Publicly Accessible Content     | Train authorized individuals to ensure that publicly accessible information does not contain CUI.   | Functional     | Intersects With   | Terms of Employment   | HRS-05   | Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.   | 5                        |  |
| 03.01.22.a    | Publicly Accessible Content     | Train authorized individuals to ensure that publicly accessible information does not contain CUI.   | Functional     | Intersects With   | Rules of Behavior   | HRS-05.1 | Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.   | 5                        |  |
| 03.01.22.a    | Publicly Accessible Content     | Train authorized individuals to ensure that publicly accessible information does not contain CUI.   | Functional     | Intersects With   | 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.   | 5                        |  |
| 03.01.22.a    | Publicly Accessible Content     | Train authorized individuals to ensure that publicly accessible information does not contain CUI.   | 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                        |  |
| 03.01.22.a    | Publicly Accessible Content     | Train authorized individuals to ensure that publicly accessible information does not contain CUI.   | Functional     | Intersects With   | 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.   | 5                        |  |
| 03.01.22.a    | Publicly Accessible Content     | Train authorized individuals to ensure that publicly accessible information does not contain CUI.   | Functional     | Intersects With   | Web Security  | WEB-01   | Mechanisms exist to facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures.  | 5                        |  |
| 03.01.22.b    | Publicly Accessible Content     | Review the content on publicly accessible systems for CUI and remove such information, if discovered.   | Functional     | Intersects With   | Publicly Accessible Content   | DCH-15   | Mechanisms exist to control publicly-accessible content.  | 5                        |  |
| 03.01.22.b    | Publicly Accessible Content     | Review the content on publicly accessible systems for CUI and remove such information, if discovered.   | Functional     | Intersects With   | Monitoring For Information Disclosure   | MON-11   | Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of non-public information.  | 5                        |  |
| 03.01.22.b    | Publicly Accessible Content     | Review the content on publicly accessible systems for CUI and remove such information, if discovered.   | Functional     | Intersects With   | Publicly Accessible Content Reviews   | WEB-14   | Mechanisms exist to routinely review the content on publicly accessible systems for sensitive/regulated data and remove such information, if discovered.  | 5                        |  |
| 03.02.01      | Literacy Training and Awareness | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.02.01.a    | Literacy Training and Awareness | Provide security literacy training to system users.   | Functional     | Subset Of         | Security, Compliance & Resilience-Minded Workforce                                | SAT-01   | Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.   | 10                       |  |
| 03.02.01.a.01 | Literacy Training and Awareness | As part of initial training for new users and [Assignment: organization-defined frequency] thereafter.  | Functional     | Intersects With   | 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.   | 8                        | ODP Value: at least every 12 months  |
| 03.02.01.a.01 | Literacy Training and Awareness | As part of initial training for new users and [Assignment: organization-defined frequency] thereafter.  | 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.   | 8                        | ODP Value: at least every 12 months  |
| 03.02.01.a.01 | Literacy Training and Awareness | As part of initial training for new users and [Assignment: organization-defined frequency] thereafter.  | Functional     | Intersects With   | 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.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.02.01.a.01 | Literacy Training and Awareness | As part of initial training for new users and [Assignment: organization-defined frequency] thereafter.  | Functional     | Intersects With   | Privileged Users  | SAT-03.5 | Mechanisms exist to provide specific training for privileged users to ensure privileged users understand their unique roles and responsibilities.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.02.01.a.01 | Literacy Training and Awareness | As part of initial training for new users and [Assignment: organization-defined frequency] thereafter.  | Functional     | Intersects With   | Cyber Threat Environment  | SAT-03.6 | Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.02.01.a.02 | Literacy Training and Awareness | When required by system changes or following [Assignment: organization-defined events], and   | Functional     | Intersects With   | 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.   | 8                        | ODP Value: significant, novel incidents, or significant changes to risks                                     |
| 03.02.01.a.02 | Literacy Training and Awareness | When required by system changes or following [Assignment: organization-defined events], and   | 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.   | 8                        | ODP Value: significant, novel incidents, or significant changes to risks                                     |
| 03.02.01.a.02 | Literacy Training and Awareness | When required by system changes or following [Assignment: organization-defined events], and   | Functional     | Intersects With   | Cyber Threat Environment  | SAT-03.6 | Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.02.01.a.02 | Literacy Training and Awareness | When required by system changes or following [Assignment: organization-defined events], and   | Functional     | Intersects With   | Threat Intelligence Feeds   | THR-03   | Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.02.01.a.03 | Literacy Training and Awareness | On recognizing and reporting indicators of insider threat, social engineering, and social mining.   | Functional     | Intersects With   | 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.   | 5                        |  |
| 03.02.01.a.03 | Literacy Training and Awareness | On recognizing and reporting indicators of insider threat, social engineering, and social mining.   | Functional     | Intersects With   | Social Engineering & Mining   | SAT-02.2 | Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.   | 5                        |  |
| 03.02.01.a.03 | Literacy Training and Awareness | On recognizing and reporting indicators of insider threat, social engineering, and social mining.   | Functional     | Intersects With   | Cyber Threat Environment  | SAT-03.6 | Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.   | 5                        |  |
| 03.02.01.a.03 | Literacy Training and Awareness | On recognizing and reporting indicators of insider threat, social engineering, and social mining.   | Functional     | Intersects With   | Threat Intelligence Feeds   | THR-03   | Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.   | 5                        |  |
| 03.02.01.a.03 | Literacy Training and Awareness | On recognizing and reporting indicators of insider threat, social engineering, and social mining.   | Functional     | Intersects With   | Insider Threat Awareness  | THR-05   | Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.  | 5                        |  |
| 03.02.01.b    | Literacy Training and Awareness | Update security literacy training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. | Functional     | Intersects With   | 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.   | 8                        | ODP Values: (01) at least every 12 months (02) significant, novel incidents, or significant changes to risks |
| 03.02.01.b    | Literacy Training and Awareness | Update security literacy training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. | Functional     | Intersects With   | Cyber Threat Environment  | SAT-03.6 | Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.02.01.b    | Literacy Training and Awareness | Update security literacy training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. | Functional     | Intersects With   | Threat Intelligence Feeds   | THR-03   | Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.02.02      | Role-Based Training             | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.02.02.a    | Role-Based Training             | Provide role-based security training to organizational personnel.   | 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                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.02.02.a.01 | Role-Based Training             | Before authorizing access to the system or CUI, before performing assigned duties, and [Assignment: organization-defined frequency] thereafter  | Functional     | Intersects With   | Roles With Special Protection Measures  | HRS-04.1 | Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.  | 5                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.02.02.a.01 | Role-Based Training             | Before authorizing access to the system or CUI, before performing assigned duties, and [Assignment: organization-defined frequency] thereafter  | Functional     | Intersects With   | Formal Indocination   | HRS-04.2 | Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access.   | 8                        | ODP Value: at least every 12 months  |
| 03.02.02.a.01 | Role-Based Training             | Before authorizing access to the system or CUI, before performing assigned duties, and [Assignment: organization-defined frequency] thereafter  | 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.   | 8                        | ODP Value: at least every 12 months  |
| 03.02.02.a.01 | Role-Based Training             | Before authorizing access to the system or CUI, before performing assigned duties, and [Assignment: organization-defined frequency] thereafter  | Functional     | Intersects With   | 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.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.02.02.a.01 | Role-Based Training             | Before authorizing access to the system or CUI, before performing assigned duties, and [Assignment: organization-defined frequency] thereafter  | Functional     | Intersects With   | Privileged Users  | SAT-03.5 | Mechanisms exist to provide specific training for privileged users to ensure privileged users understand their unique roles and responsibilities.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.02.02.a.01 | Role-Based Training             | Before authorizing access to the system or CUI, before performing assigned duties, and [Assignment: organization-defined frequency] thereafter  | Functional     | Intersects With   | Cyber Threat Environment  | SAT-03.6 | Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.   | 5                        | DoD-provided ODP does not apply to this specific 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   |   |   |
|---------------|-------------------------|--|----------------|-------------------|---|----------|--|--------------------------|---|---|---|
| 03.02.02.a.02 | Role-Based Training     | When required by system changes or following [Assignment: organization-defined events].  | Functional     | Intersects With   | Role-Based Security, Compliance & Resilience Training | SAT-03   | Mechanisms exist to provide role-based security, compliance and resilience-related training:<br>(1) Before authorizing access to the system or performing assigned duties;<br>(2) When required by system changes; and<br>(3) Annually thereafter.   | 8                        | ODP Value: significant, novel incidents, or significant changes to risks  |   |   |
| 03.02.02.a.02 | Role-Based Training     | When required by system changes or following [Assignment: organization-defined events].  | Functional     | Intersects With   | Cyber Threat Environment                              | SAT-03.6 | Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.  | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |   |   |
| 03.02.02.b    | Role-Based Training     | Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. | Functional     | Intersects With   | Role-Based Security, Compliance & Resilience Training | SAT-03   | Mechanisms exist to provide role-based security, compliance and resilience-related training:<br>(1) Before authorizing access to the system or performing assigned duties;<br>(2) When required by system changes; and<br>(3) Annually thereafter.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |   |   |
| 03.02.02.b    | Role-Based Training     | Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. | Functional     | Intersects With   | Cyber Threat Environment                              | SAT-03.6 | Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.  | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |   |   |
| 03.02.02.b    | Role-Based Training     | Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. | Functional     | Intersects With   | Threat Intelligence Feeds                             | THR-03   | Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.  | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |   |   |
| 03.02.03      | Withdrawn               | Incorporated into 03.02.01.  | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control   |   |   |
| 03.03.01      | Event Logging           | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control   |   |   |
| 03.03.01.a    | Event Logging           | Specify the following event types selected for logging within the system: [Assignment: organization-defined event types].                | Functional     | Subset Of         | Continuous Monitoring                                 | MON-01   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.  | 10                       | DoD-provided ODP does not apply to this specific SCF control.   |   |   |
| 03.03.01.a    | Event Logging           | Specify the following event types selected for logging within the system: [Assignment: organization-defined event types].                | Functional     | Intersects With   | 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.  | 8                        | ODP Values: at a minimum and where applicable:<br>(1) Authentication events:<br>(a) Logons (Success/Failure)<br>(b) Logoffs (Success)<br>(2) Security Relevant File and Objects events:<br>(a) Create (Success/Failure)<br>(b) Access (Success/Failure)<br>(c) Delete (Success/Failure)<br>(d) Modify (Success/Failure)<br>(e) Permission Modification (Success/Failure)<br>(f) Ownership Modification (Success/Failure)<br>(3) Export/Writes/downloads to devices/digital media (e.g., CD/DVD, USB, SD) (Success/Failure)<br>(4) Import/Uploads from devices/digital media (e.g., CD/DVD, USB, SD) (Success/Failure)<br>(5) User and Group Management events:<br>(a) User add, delete, modify, disable, lock (Success/Failure)<br>(b) Group/Role add, delete, modify (Success/Failure)<br>(6) User of Privileged/Special Rights events:<br>(a) Security or audit policy changes (Success/Failure)<br>(b) Configuration changes (Success/Failure)<br>(7) Admin or root-level access (Success/Failure)<br>(8) Privilege/Role escalation (Success/Failure)<br>(9) Audit and security relevant log data accesses (Success/Failure)<br>(10) System reboot, restart, and shutdown (Success/Failure)<br>(11) Print to a device (Success/Failure)<br>(12) Print to a file (e.g., pdf format) (Success/Failure)<br>(13) Application (e.g., Adobe, Firefox, MS Office Suite) initialization (Success/Failure)<br>For additional guidance, see: OMB21-31 ML 1 | 8 | DoD-provided ODP does not apply to this specific SCF control. |
| 03.03.01.a    | Event Logging           | Specify the following event types selected for logging within the system: [Assignment: organization-defined event types].                | Functional     | Intersects With   | 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.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |   |   |
| 03.03.01.a    | Event Logging           | Specify the following event types selected for logging within the system: [Assignment: organization-defined event types].                | Functional     | Intersects With   | 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:<br>(1) Establish what type of event occurred;<br>(2) When (date and time) the event occurred;<br>(3) Where the event occurred;<br>(4) The source of the event;<br>(5) The outcome (success or failure) of the event; and<br>(6) The identity of any user/subject associated with the event. | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |   |   |
| 03.03.01.a    | Event Logging           | Specify the following event types selected for logging within the system: [Assignment: organization-defined event types].                | Functional     | Intersects With   | Audit Trails  | MON-03.2 | Mechanisms exist to link system access to individual users or service accounts.  | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |   |   |
| 03.03.01.b    | Event Logging           | Review and update the event types selected for logging [Assignment: organization-defined frequency].                                     | 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                       | ODP Value: at least every 12 months and after any significant incidents or significant changes to risks   |   |   |
| 03.03.01.b    | Event Logging           | Review and update the event types selected for logging [Assignment: organization-defined frequency].                                     | Functional     | Intersects With   | Central Review & Analysis                             | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |   |   |
| 03.03.02      | Audit Record Content    | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control   |   |   |
| 03.03.02.a    | Audit Record Content    | Include the following content in audit records:  | Functional     | Intersects With   | 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:<br>(1) Establish what type of event occurred;<br>(2) When (date and time) the event occurred;<br>(3) Where the event occurred;<br>(4) The source of the event;<br>(5) The outcome (success or failure) of the event; and<br>(6) The identity of any user/subject associated with the event. | 5                        |   |   |   |
| 03.03.02.a.01 | Audit Record Content    | What type of event occurred  | Functional     | Intersects With   | 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:<br>(1) Establish what type of event occurred;<br>(2) When (date and time) the event occurred;<br>(3) Where the event occurred;<br>(4) The source of the event;<br>(5) The outcome (success or failure) of the event; and<br>(6) The identity of any user/subject associated with the event. | 5                        |   |   |   |
| 03.03.02.a.02 | Audit Record Content    | When the event occurred  | Functional     | Intersects With   | 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:<br>(1) Establish what type of event occurred;<br>(2) When (date and time) the event occurred;<br>(3) Where the event occurred;<br>(4) The source of the event;<br>(5) The outcome (success or failure) of the event; and<br>(6) The identity of any user/subject associated with the event. | 5                        |   |   |   |
| 03.03.02.a.02 | Audit Record Content    | When the event occurred  | 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                        |   |   |   |
| 03.03.02.a.03 | Audit Record Content    | Where the event occurred   | Functional     | Intersects With   | 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:<br>(1) Establish what type of event occurred;<br>(2) When (date and time) the event occurred;<br>(3) Where the event occurred;<br>(4) The source of the event;<br>(5) The outcome (success or failure) of the event; and<br>(6) The identity of any user/subject associated with the event. | 5                        |   |   |   |
| 03.03.02.a.04 | Audit Record Content    | Source of the event  | Functional     | Intersects With   | 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:<br>(1) Establish what type of event occurred;<br>(2) When (date and time) the event occurred;<br>(3) Where the event occurred;<br>(4) The source of the event;<br>(5) The outcome (success or failure) of the event; and<br>(6) The identity of any user/subject associated with the event. | 5                        |   |   |   |
| 03.03.02.a.05 | Audit Record Content    | Outcome of the event   | Functional     | Intersects With   | 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:<br>(1) Establish what type of event occurred;<br>(2) When (date and time) the event occurred;<br>(3) Where the event occurred;<br>(4) The source of the event;<br>(5) The outcome (success or failure) of the event; and<br>(6) The identity of any user/subject associated with the event. | 5                        |   |   |   |
| 03.03.02.a.06 | Audit Record Content    | Identity of the individuals, subjects, objects, or entities associated with the event  | Functional     | Intersects With   | 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:<br>(1) Establish what type of event occurred;<br>(2) When (date and time) the event occurred;<br>(3) Where the event occurred;<br>(4) The source of the event;<br>(5) The outcome (success or failure) of the event; and<br>(6) The identity of any user/subject associated with the event. | 5                        |   |   |   |
| 03.03.02.b    | Audit Record Content    | Provide additional information for audit records as needed.  | Functional     | Intersects With   | 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:<br>(1) Mission / business functions;<br>(2) Operational environment;<br>(3) Specific threats or vulnerabilities; or<br>(4) Other conditions or situations that could affect mission / business success.   | 5                        |   |   |   |
| 03.03.02.b    | Audit Record Content    | Provide additional information for audit records as needed.  | Functional     | Intersects With   | 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:<br>(1) Establish what type of event occurred;<br>(2) When (date and time) the event occurred;<br>(3) Where the event occurred;<br>(4) The source of the event;<br>(5) The outcome (success or failure) of the event; and<br>(6) The identity of any user/subject associated with the event. | 5                        |   |   |   |
| 03.03.03      | Audit Record Generation | 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   |
|------------|--|---|----------------|-------------------|--|-----------|--|--------------------------|---|
| 03.03.03.a | Audit Record Generation                      | Generate audit records for the selected event types and audit record content specified in 03.03.01 and 03.03.02.  | 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                       |   |
| 03.03.03.b | Audit Record Generation                      | Retain audit records for a time period consistent with the records retention policy.  | Functional     | Intersects With   | Protection of Event Logs   | MON-08    | Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.  | 5                        |   |
| 03.03.03.b | Audit Record Generation                      | Retain audit records for a time period consistent with the records retention policy.  | 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                       |   |
| 03.03.04   | Response to Audit Logging Process Failures   | N/A   | Functional     | No Relationship   | N/A  | N/A       | N/A  | 0                        | No applicable SCF control   |
| 03.03.04.a | Response to Audit Logging Process Failures   | Alert organizational personnel or roles within [Assignment: organization-defined time period] in the event of an audit logging process failure.   | Functional     | Intersects With   | Automated Alerts   | MON-01.12 | Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.   | 8                        | ODP Value: near real time or as soon as practicable upon discovery  |
| 03.03.04.b | Response to Audit Logging Process Failures   | Take the following additional actions: [Assignment: organization-defined additional actions].   | Functional     | Intersects With   | Incident Handling  | IRO-02    | Mechanisms exist to cover:<br>1) Preparation;<br>2) Automated event detection or manual incident report intake;<br>3) Analysis;<br>4) Containment;<br>5) Eradication; and<br>6) Recovery.  | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.03.04.b | Response to Audit Logging Process Failures   | Take the following additional actions: [Assignment: organization-defined additional actions].   | Functional     | Intersects With   | 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.  | 8                        | ODP Value: document the failure and resolution, troubleshoot, repair/restart the audit logging process, and report as incident if applicable  |
| 03.03.05   | Audit Record Review, Analysis, and Reporting | N/A   | Functional     | No Relationship   | N/A  | N/A       | N/A  | 0                        | No applicable SCF control   |
| 03.03.05.a | Audit Record Review, Analysis, and Reporting | Review and analyze system audit records [Assignment: organization-defined frequency] for indications and the potential impact of inappropriate or unusual activity.   | 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 priorities.  | 10                       | ODP Value: at least weekly  |
| 03.03.05.a | Audit Record Review, Analysis, and Reporting | Review and analyze system audit records [Assignment: organization-defined frequency] for indications and the potential impact of inappropriate or unusual activity.   | 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.   | 3                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.03.05.a | Audit Record Review, Analysis, and Reporting | Review and analyze system audit records [Assignment: organization-defined frequency] for indications and the potential impact of inappropriate or unusual activity.   | 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                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.03.05.a | Audit Record Review, Analysis, and Reporting | Review and analyze system audit records [Assignment: organization-defined frequency] for indications and the potential impact of inappropriate or unusual activity.   | Functional     | Intersects With   | Central Review & Analysis  | MON-02.2  | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.   | 3                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.03.05.a | Audit Record Review, Analysis, and Reporting | Review and analyze system audit records [Assignment: organization-defined frequency] for indications and the potential impact of inappropriate or unusual activity.   | Functional     | Intersects With   | Anomalous Behavior   | MON-16    | Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.  | 8                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.03.05.b | Audit Record Review, Analysis, and Reporting | Report findings to organizational personnel or roles.   | Functional     | Intersects With   | Automated Alerts   | MON-01.12 | Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.   | 8                        |   |
| 03.03.05.b | Audit Record Review, Analysis, and Reporting | Report findings to organizational personnel or roles.   | 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.  | 8                        |   |
| 03.03.05.c | Audit Record Review, Analysis, and Reporting | Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.  | 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.   | 8                        |   |
| 03.03.05.c | Audit Record Review, Analysis, and Reporting | Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.  | Functional     | Intersects With   | Correlate Monitoring Information   | MON-02.1  | Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.   | 8                        |   |
| 03.03.05.c | Audit Record Review, Analysis, and Reporting | Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.  | Functional     | Intersects With   | Central Review & Analysis  | MON-02.2  | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.   | 5                        |   |
| 03.03.05.c | Audit Record Review, Analysis, and Reporting | Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.  | Functional     | Intersects With   | Integration of Scanning & Other Monitoring Information                               | MON-02.3  | Automated mechanisms exist to integrate the analysis of audit records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further enhance the ability to identify inappropriate or unusual activity.  | 5                        |   |
| 03.03.06   | Audit Record Reduction and Report Generation | N/A   | Functional     | No Relationship   | N/A  | N/A       | N/A  | 0                        | No applicable SCF control   |
| 03.03.06.a | Audit Record Reduction and Report Generation | Implement an audit record reduction and report generation capability that supports audit review, analysis, reporting requirements, and after-the-fact investigations of incidents.  | 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                        |   |
| 03.03.06.b | Audit Record Reduction and Report Generation | Preserve the original content and time ordering of audit records.   | Functional     | Equal             | Protection of Event Logs   | MON-08    | Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.  | 10                       |   |
| 03.03.07   | Time Stamps                                  | N/A   | Functional     | No Relationship   | N/A  | N/A       | N/A  | 0                        | No applicable SCF control   |
| 03.03.07.a | Time Stamps                                  | Use internal system clocks to generate time stamps for audit records.   | Functional     | Subset Of         | 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.   | 10                       |   |
| 03.03.07.b | Time Stamps                                  | Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time (UTC), have a fixed local time offset from UTC, or include the local time offset as part of the time stamp. | Functional     | Subset Of         | Synchronization With Authoritative Time Source                                       | MON-07.1  | Mechanisms exist to synchronize internal system clocks with an authoritative time source.  | 10                       | ODP Value: a granularity of one (1) second or smaller   |
| 03.03.08   | Protection of Audit Information              | N/A   | Functional     | No Relationship   | N/A  | N/A       | N/A  | 0                        | No applicable SCF control   |
| 03.03.08.a | Protection of Audit Information              | Protect audit information and audit logging tools from unauthorized access, modification, and deletion.   | Functional     | Intersects With   | Protection of Event Logs   | MON-08    | Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.  | 5                        |   |
| 03.03.08.a | Protection of Audit Information              | Protect audit information and audit logging tools from unauthorized access, modification, and deletion.   | Functional     | Intersects With   | Event Log Backup on Separate Physical Systems / Components                           | MON-08.1  | Mechanisms exist to back up event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or similar automated tool.   | 5                        |   |
| 03.03.08.a | Protection of Audit Information              | Protect audit information and audit logging tools from unauthorized access, modification, and deletion.   | Functional     | Intersects With   | 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.   | 5                        |   |
| 03.03.08.a | Protection of Audit Information              | Protect audit information and audit logging tools from unauthorized access, modification, and deletion.   | Functional     | Intersects With   | Cryptographic Protection of Event Log Information                                    | MON-08.3  | Cryptographic mechanisms exist to protect the integrity of event logs and audit tools.   | 5                        |   |
| 03.03.08.a | Protection of Audit Information              | Protect audit information and audit logging tools from unauthorized access, modification, and deletion.   | 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.  | 8                        |   |
| 03.03.08.b | Protection of Audit Information              | Authorize access to management of audit logging functionality to only a subset of privileged users or roles.  | Functional     | Equal             | Access by Subset of Privileged Users   | MON-08.2  | Mechanisms exist to restrict access to the management of event logs to privileged users with a specific business need.   | 10                       |   |
| 03.03.08.b | Protection of Audit Information              | Authorize access to management of audit logging functionality to only a subset of privileged users or 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                       |   |
| 03.03.08.b | Protection of Audit Information              | Authorize access to management of audit logging functionality to only a subset of privileged users or roles.  | 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.  | 8                        |   |
| 03.03.09   | Withdrawn                                    | Incorporated into 03.03.08.   | Functional     | No Relationship   | N/A  | N/A       | N/A  | 0                        | No applicable SCF control   |
| 03.04.01   | Baseline Configuration                       | N/A   | Functional     | No Relationship   | N/A  | N/A       | N/A  | 0                        | No applicable SCF control   |
| 03.04.01.a | Baseline Configuration                       | Develop and maintain under configuration control, a current baseline configuration of the system.   | Functional     | Subset Of         | Configuration Management Program   | CFG-01    | Mechanisms exist to facilitate the implementation of configuration management controls.  | 10                       |   |
| 03.04.01.a | Baseline Configuration                       | Develop and maintain under configuration control, a current baseline configuration of the 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                        |   |
| 03.04.01.a | Baseline Configuration                       | Develop and maintain under configuration control, a current baseline configuration of the system.   | Functional     | Intersects With   | Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas | CFG-02.5  | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.  | 5                        |   |
| 03.04.01.a | Baseline Configuration                       | Develop and maintain under configuration control, a current baseline configuration of the system.   | Functional     | Intersects With   | Approved Configuration Deviations  | CFG-02.7  | Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.   | 5                        |   |
| 03.04.01.a | Baseline Configuration                       | Develop and maintain under configuration control, a current baseline configuration of the system.   | Functional     | Intersects With   | 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:<br>(1) Mission / business functions;<br>(2) Operational environment;<br>(3) Specific threats or vulnerabilities; or<br>(4) Other conditions or situations that could affect mission / business success. | 5                        |   |
| 03.04.01.b | Baseline Configuration                       | Review and update the baseline configuration of the system [Assignment: organization-defined frequency] and when system components are installed or modified.   | Functional     | Intersects With   | Reviews & Updates  | CFG-02.1  | Mechanisms exist to review and update baseline configurations:<br>(1) At least annually;<br>(2) When required due to so; or<br>(3) As part of system component installations and upgrades.   | 8                        | ODP Value: at least every 12 months and after any significant incidents or significant changes occur  |
| 03.04.02   | Configuration Settings                       | N/A   | Functional     | No Relationship   | N/A  | N/A       | N/A  | 0                        | No applicable SCF control   |
| 03.04.02.a | Configuration Settings                       | Establish, document, and implement the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements: [Assignment: organization-defined configuration settings].                                    | 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.  | 8                        | ODP Value: Apply the appropriate use of common security configurations available from the National Institute of Standards and Technology's National Checklist Program (NCP) website ( <a href="https://nsc.nist.gov/repository">https://nsc.nist.gov/repository</a> ) and prevent remote devices from simultaneously establishing nonremote connections with organizational systems and communicating via some other unauthorized connection to resources in external networks. Document any deviations from the published standard or source document. |
| 03.04.02.a | Configuration Settings                       | Establish, document, and implement the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements: [Assignment: organization-defined configuration settings].                                    | Functional     | Intersects With   | Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas | CFG-02.5  | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.  | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.04.02.a | Configuration Settings                       | Establish, document, and implement the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements: [Assignment: organization-defined configuration settings].                                    | Functional     | Intersects With   | 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:<br>(1) Mission / business functions;<br>(2) Operational environment;<br>(3) Specific threats or vulnerabilities; or<br>(4) Other conditions or situations that could affect mission / business success. | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.04.02.a | Configuration Settings                       | Establish, document, and implement the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements: [Assignment: organization-defined configuration settings].                                    | Functional     | Intersects With   | 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.  | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.04.02.a | Configuration Settings                       | Establish, document, and implement the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements: [Assignment: organization-defined configuration settings].                                    | Functional     | Intersects With   | Configuration Enforcement  | CFG-06    | Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.  | 5                        | DoD-provided ODP does not apply to this specific 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  |
|------------|--|--|----------------|-------------------|--|----------|---|--------------------------|--|
| 03.04.02.b | Configuration Settings                   | Identify, document, and approve any deviations from established configuration settings.  | Functional     | Intersects With   | Approved Baseline Deviations   | AST-02.4 | Mechanisms exist to document and govern instances of approved deviations from established baseline configurations.  | 5                        |  |
| 03.04.02.b | Configuration Settings                   | Identify, document, and approve any deviations from established configuration settings.  | Functional     | Intersects With   | Reviews & Updates  | CFG-02.1 | Mechanisms exist to review and update baseline configurations:<br>(1) At least annually.<br>(2) When required due to so; or<br>(3) As part of system component installations and upgrades.  | 5                        |  |
| 03.04.02.b | Configuration Settings                   | Identify, document, and approve any deviations from established configuration settings.  | 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.  | 3                        |  |
| 03.04.02.b | Configuration Settings                   | Identify, document, and approve any deviations from established configuration settings.  | Functional     | Intersects With   | Approved Configuration Deviations  | CFG-02.7 | Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.  | 5                        |  |
| 03.04.02.b | Configuration Settings                   | Identify, document, and approve any deviations from established configuration settings.  | Functional     | Intersects With   | 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:<br>(1) Mission / business functions;<br>(2) Operational environment;<br>(3) Specific threats or vulnerabilities; or<br>(4) Other conditions or situations that could affect mission / business success.  | 5                        |  |
| 03.04.02.b | Configuration Settings                   | Identify, document, and approve any deviations from established configuration settings.  | Functional     | Intersects With   | Configuration Enforcement  | CFG-06   | Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.   | 3                        |  |
| 03.04.02.b | Configuration Settings                   | Identify, document, and approve any deviations from established configuration settings.  | Functional     | Subset Of         | Change Management Program  | CHG-01   | Mechanisms exist to facilitate the implementation of a change management program.   | 10                       |  |
| 03.04.02.b | Configuration Settings                   | Identify, document, and approve any deviations from established configuration settings.  | Functional     | Intersects With   | Configuration Change Control   | CHG-02   | Mechanisms exist to govern the technical configuration change control processes.  | 5                        |  |
| 03.04.02.b | Configuration Settings                   | Identify, document, and approve any deviations from established configuration settings.  | Functional     | Intersects With   | Prohibition Of Changes   | CHG-02.1 | Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.   | 5                        |  |
| 03.04.02.b | Configuration Settings                   | Identify, document, and approve any deviations from established configuration settings.  | 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                        |  |
| 03.04.03   | Configuration Change Control             | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.04.03.a | Configuration Change Control             | Define the types of changes to the system that are configuration-controlled.   | Functional     | Intersects With   | Configuration Enforcement  | CFG-06   | Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.   | 5                        |  |
| 03.04.03.a | Configuration Change Control             | Define the types of changes to the system that are configuration-controlled.   | Functional     | Subset Of         | Change Management Program  | CHG-01   | Mechanisms exist to facilitate the implementation of a change management program.   | 10                       |  |
| 03.04.03.a | Configuration Change Control             | Define the types of changes to the system that are configuration-controlled.   | Functional     | Intersects With   | Configuration Change Control   | CHG-02   | Mechanisms exist to govern the technical configuration change control processes.  | 5                        |  |
| 03.04.03.a | Configuration Change Control             | Define the types of changes to the system that are configuration-controlled.   | Functional     | Intersects With   | Prohibition Of Changes   | CHG-02.1 | Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.   | 5                        |  |
| 03.04.03.b | Configuration Change Control             | Review proposed configuration-controlled changes to the system, and approve or disapprove such changes with explicit consideration for security impacts.                                     | Functional     | Intersects With   | Configuration Change Control   | CHG-02   | Mechanisms exist to govern the technical configuration change control processes.  | 5                        |  |
| 03.04.03.b | Configuration Change Control             | Review proposed configuration-controlled changes to the system, and approve or disapprove such changes with explicit consideration for security impacts.                                     | Functional     | Intersects With   | Test, Validate & Document Changes  | CHG-02.2 | Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.  | 5                        |  |
| 03.04.03.b | Configuration Change Control             | Review proposed configuration-controlled changes to the system, and approve or disapprove such changes with explicit consideration for security impacts.                                     | Functional     | Intersects With   | Security Impact Analysis for Changes   | CHG-03   | Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.   | 5                        |  |
| 03.04.03.c | Configuration Change Control             | Implement and document approved configuration-controlled changes to the system.  | Functional     | Intersects With   | Test, Validate & Document Changes  | CHG-02.2 | Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.  | 5                        |  |
| 03.04.03.c | Configuration Change Control             | Implement and document approved configuration-controlled changes to the system.  | Functional     | Intersects With   | Configuration Change Control   | CHG-02   | Mechanisms exist to govern the technical configuration change control processes.  | 5                        |  |
| 03.04.03.c | Configuration Change Control             | Implement and document approved configuration-controlled changes to the system.  | Functional     | Intersects With   | Maintenance Operations   | MNT-01   | Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.  | 3                        |  |
| 03.04.03.c | Configuration Change Control             | Implement and document approved configuration-controlled changes to the system.  | Functional     | Intersects With   | Controlled Maintenance   | MNT-02   | Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).  | 3                        |  |
| 03.04.03.d | Configuration Change Control             | Monitor and review activities associated with configuration-controlled changes to the system.  | Functional     | Subset Of         | 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.  | 10                       |  |
| 03.04.04   | Impact Analyses                          | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.04.04.a | Impact Analyses                          | Analyze changes to the system to determine potential security impacts prior to change implementation.  | Functional     | Intersects With   | Test, Validate & Document Changes  | CHG-02.2 | Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.  | 3                        |  |
| 03.04.04.a | Impact Analyses                          | Analyze changes to the system to determine potential security impacts prior to change implementation.  | Functional     | Intersects With   | Security, Compliance & Resilience Representative for Asset Lifecycle Changes         | CHG-02.3 | Mechanisms exist to include a cybersecurity and/or data protection representative in the configuration change control review process.   | 8                        |  |
| 03.04.04.a | Impact Analyses                          | Analyze changes to the system to determine potential security impacts prior to change implementation.  | Functional     | Intersects With   | Security Impact Analysis for Changes   | CHG-03   | Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.   | 8                        |  |
| 03.04.04.b | Impact Analyses                          | Verify that the security requirements for the system continue to be satisfied after the system changes have been implemented.  | 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                       |  |
| 03.04.05   | Access Restrictions for Change           | Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.   | Functional     | Intersects With   | Access Restriction For Change  | CHG-04   | Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.   | 5                        |  |
| 03.04.05   | Access Restrictions for Change           | Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.   | Functional     | Intersects With   | Permissions To Implement Changes   | CHG-04.4 | Mechanisms exist to limit operational privileges for implementing changes.  | 5                        |  |
| 03.04.05   | Access Restrictions for Change           | Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.   | Functional     | Intersects With   | 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.  | 5                        |  |
| 03.04.05   | Access Restrictions for Change           | Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.   | 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                        |  |
| 03.04.06   | Least Functionality                      | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.04.06.a | Least Functionality                      | Configure the system to provide only mission-essential capabilities.   | 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.   | 8                        |  |
| 03.04.06.a | Least Functionality                      | Configure the system to provide only mission-essential capabilities.   | Functional     | Intersects With   | Approved Baseline Deviations   | AST-02.4 | Mechanisms exist to document and govern instances of approved deviations from established baseline configurations.  | 3                        |  |
| 03.04.06.a | Least Functionality                      | Configure the system to provide only mission-essential capabilities.   | Functional     | Intersects With   | Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas | CFG-02.5 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.   | 8                        |  |
| 03.04.06.a | Least Functionality                      | Configure the system to provide only mission-essential capabilities.   | Functional     | Intersects With   | 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:<br>(1) Mission / business functions;<br>(2) Operational environment;<br>(3) Specific threats or vulnerabilities; or<br>(4) Other conditions or situations that could affect mission / business success.  | 3                        |  |
| 03.04.06.a | Least Functionality                      | Configure the system to provide only mission-essential capabilities.   | Functional     | Equal             | Least Functionality  | CFG-03   | Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.   | 10                       |  |
| 03.04.06.b | Least Functionality                      | Prohibit or restrict use of the following functions, ports, protocols, connections, and services: (Assignment: organization-defined functions, ports, protocols, connections, and 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                       | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.04.06.b | Least Functionality                      | Prohibit or restrict use of the following functions, ports, protocols, connections, and services: (Assignment: organization-defined functions, ports, protocols, connections, and services). | Functional     | Subset Of         | Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas | CFG-02.5 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.   | 10                       | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.04.06.b | Least Functionality                      | Prohibit or restrict use of the following functions, ports, protocols, connections, and services: (Assignment: organization-defined functions, ports, protocols, connections, and services). | Functional     | Equal             | Least Functionality  | CFG-03   | Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.   | 10                       | ODP Value: Guidance: Where feasible, organizations should limit component functionality to a single function per component. Organizations should consider removing unused or unnecessary software and disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of components, transfer of information, and tunneling. Organizations should employ network scanning tools, intrusion detection and prevention systems, and endpoint protection technologies, such as firewalls and host-based intrusion detection systems, to identify and prevent the use of prohibited functions, protocols, ports, and services. Least functionality should also be achieved as part of the fundamental design and development of the system. |
| 03.04.06.c | Least Functionality                      | Review the system (Assignment: organization-defined frequency) to identify unnecessary or nonsecure functions, ports, protocols, connections, and services.                                  | Functional     | Equal             | Periodic Review  | CFG-03.1 | Mechanisms exist to periodically review system configurations to identify and disable unnecessary and non-secure functions, ports, protocols, and services.   | 10                       | ODP Value: at least every 12 months, when any significant functions, ports, protocols, or services changes are made, and after any system incidents or significant changes to risks  |
| 03.04.06.d | Least Functionality                      | Disable or remove functions, ports, protocols, connections, and services that are unnecessary or nonsecure.  | 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                       |  |
| 03.04.06.d | Least Functionality                      | Disable or remove functions, ports, protocols, connections, and services that are unnecessary or nonsecure.  | Functional     | Subset Of         | Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas | CFG-02.5 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.   | 10                       |  |
| 03.04.06.d | Least Functionality                      | Disable or remove functions, ports, protocols, connections, and services that are unnecessary or nonsecure.  | Functional     | Equal             | Least Functionality  | CFG-03   | Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.   | 10                       |  |
| 03.04.07   | Withdrawn                                | Incorporated into 03.04.06 and 03.04.08.   | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.04.08   | Authorized Software - Allow by Exception | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.04.08.a | Authorized Software - Allow by Exception | Identify software programs authorized to execute on the system.  | Functional     | Subset Of         | Asset Inventories  | AST-02   | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:<br>(1) Accurately reflects the current TAASD in use;<br>(2) Identifies authorized software products, including business justification details;<br>(3) Is at the level of granularity deemed necessary for tracking and reporting;<br>(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and<br>(5) Is available for review and audit by designated organizational personnel. | 10                       |  |
| 03.04.08.a | Authorized Software - Allow by Exception | Identify software programs authorized to execute on the system.  | Functional     | Intersects With   | Configuration Management Database (CMDB)   | AST-02.9 | Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.  | 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   |
|------------|--|---|----------------|-------------------|--|----------|--|--------------------------|---|
| 03.04.08.a | Authorized Software - Allow by Exception | Identify software programs authorized to execute on the system.   | Functional     | Intersects With   | 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:<br>(1) Mission / business functions;<br>(2) Operational environment;<br>(3) Specific threats or vulnerabilities; or<br>(4) Other conditions or situations that could affect mission / business success.   | 8                        |   |
| 03.04.08.a | Authorized Software - Allow by Exception | Identify software programs authorized to execute on the system.   | Functional     | Intersects With   | 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.  | 8                        |   |
| 03.04.08.a | Authorized Software - Allow by Exception | Identify software programs authorized to execute on the system.   | Functional     | Intersects With   | Explicitly Allow / Deny Applications                               | CFG-03.3 | Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.   | 5                        |   |
| 03.04.08.b | Authorized Software - Allow by Exception | Implement a deny-all, allow-by-exception policy for the execution of authorized software programs on the system.      | Functional     | Intersects With   | Prevent Unauthorized Software Execution                            | CFG-03.2 | Mechanisms exist to configure systems to prevent the execution of unauthorized software programs.  | 5                        |   |
| 03.04.08.b | Authorized Software - Allow by Exception | Implement a deny-all, allow-by-exception policy for the execution of authorized software programs on the system.      | Functional     | Intersects With   | Explicitly Allow / Deny Applications                               | CFG-03.3 | Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.   | 5                        |   |
| 03.04.08.c | Authorized Software - Allow by Exception | Review and update the list of authorized software programs [Assignment: organization-defined frequency].              | Functional     | Intersects With   | Asset Inventories  | AST-02   | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:<br>(1) Accurately reflects the current TAASD in use;<br>(2) Identifies authorized software products, including business justification details;<br>(3) Is at the level of granularity deemed necessary for tracking and reporting;<br>(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and<br>(5) Is available for review and audit by designated organizational personnel.  | 8                        | ODP Value: at least quarterly                                 |
| 03.04.08.c | Authorized Software - Allow by Exception | Review and update the list of authorized software programs [Assignment: organization-defined frequency].              | Functional     | Intersects With   | 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.  | 8                        | DoD-provided ODP does not apply to this specific SCF control. |
| 03.04.08.c | Authorized Software - Allow by Exception | Review and update the list of authorized software programs [Assignment: organization-defined frequency].              | 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.   | 8                        | DoD-provided ODP does not apply to this specific SCF control. |
| 03.04.09   | Withdrawn                                | Addressed by 03.01.05, 03.01.06, 03.01.07, 03.04.08, and 03.12.03.  | Functional     | No Relationship   | N/A  | N/A      | N/A  | 0                        | No applicable SCF control                                     |
| 03.04.10   | System Component Inventory               | N/A   | Functional     | No Relationship   | N/A  | N/A      | N/A  | 0                        | No applicable SCF control                                     |
| 03.04.10.a | System Component Inventory               | Develop and document an inventory of system components.   | Functional     | Subset Of         | Asset Inventories  | AST-02   | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:<br>(1) Accurately reflects the current TAASD in use;<br>(2) Identifies authorized software products, including business justification details;<br>(3) Is at the level of granularity deemed necessary for tracking and reporting;<br>(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and<br>(5) Is available for review and audit by designated organizational personnel.  | 10                       |   |
| 03.04.10.a | System Component Inventory               | Develop and document an inventory of system components.   | Functional     | Intersects With   | Updates During Installations / Removals                            | AST-02.1 | Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades.  | 8                        |   |
| 03.04.10.a | System Component Inventory               | Develop and document an inventory of system components.   | Functional     | Intersects With   | Configuration Management Database (CMDB)                           | AST-02.9 | Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.   | 3                        |   |
| 03.04.10.b | System Component Inventory               | Review and update the system component inventory [Assignment: organization-defined frequency].                        | Functional     | Subset Of         | Asset Inventories  | AST-02   | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:<br>(1) Accurately reflects the current TAASD in use;<br>(2) Identifies authorized software products, including business justification details;<br>(3) Is at the level of granularity deemed necessary for tracking and reporting;<br>(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and<br>(5) Is available for review and audit by designated organizational personnel.  | 10                       | ODP Value: at least quarterly                                 |
| 03.04.10.b | System Component Inventory               | Review and update the system component inventory [Assignment: organization-defined frequency].                        | Functional     | Intersects With   | Updates During Installations / Removals                            | AST-02.1 | Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades.  | 8                        | DoD-provided ODP does not apply to this specific SCF control. |
| 03.04.10.b | System Component Inventory               | Review and update the system component inventory [Assignment: organization-defined frequency].                        | Functional     | Intersects With   | Configuration Management Database (CMDB)                           | AST-02.9 | Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.   | 3                        | DoD-provided ODP does not apply to this specific SCF control. |
| 03.04.10.c | System Component Inventory               | Update the system component inventory as part of installations, removals, and system updates.                         | Functional     | Equal             | Updates During Installations / Removals                            | AST-02.1 | Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades.  | 10                       |   |
| 03.04.10.c | System Component Inventory               | Update the system component inventory as part of installations, removals, and system updates.                         | Functional     | Intersects With   | Configuration Management Database (CMDB)                           | AST-02.9 | Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.   | 8                        |   |
| 03.04.11   | Information Location                     | N/A   | Functional     | No Relationship   | N/A  | N/A      | N/A  | 0                        | No applicable SCF control                                     |
| 03.04.11.a | Information Location                     | Identify and document the location of CUI and the system components on which the information is processed and stored. | Functional     | Subset Of         | Asset Governance   | AST-01   | Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.  | 10                       |   |
| 03.04.11.a | Information Location                     | Identify and document the location of CUI and the system components on which the information is processed and stored. | Functional     | Intersects With   | Asset Inventories  | AST-02   | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:<br>(1) Accurately reflects the current TAASD in use;<br>(2) Identifies authorized software products, including business justification details;<br>(3) Is at the level of granularity deemed necessary for tracking and reporting;<br>(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and<br>(5) Is available for review and audit by designated organizational personnel.  | 8                        |   |
| 03.04.11.a | Information Location                     | Identify and document the location of CUI and the system components on which the information is processed and stored. | Functional     | Intersects With   | Data Action Mapping  | AST-02.8 | Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive/regulatory data is stored, transmitted or processed.   | 8                        |   |
| 03.04.11.a | Information Location                     | Identify and document the location of CUI and the system components on which the information is processed and stored. | Functional     | Intersects With   | Network Diagrams & Data Flow Diagrams (DFDs)                       | AST-04   | Mechanisms exist to maintain network architecture diagrams that:<br>(1) Contain sufficient detail to assess the security of the network's architecture;<br>(2) Reflect the current architecture of the network environment; and<br>(3) Document all sensitive/regulatory data flows.   | 8                        |   |
| 03.04.11.a | Information Location                     | Identify and document the location of CUI and the system components on which the information is processed and stored. | Functional     | Intersects With   | Asset Scope Classification   | AST-04.1 | Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).  | 5                        |   |
| 03.04.11.a | Information Location                     | Identify and document the location of CUI and the system components on which the information is processed and stored. | Functional     | Intersects With   | Control Applicability Boundary Graphical Representation            | AST-04.2 | Mechanisms exist to ensure control applicability is appropriately-determined for Technology Assets, Applications and/or Services (TAAS) and third parties by graphically representing applicable boundaries.   | 5                        |   |
| 03.04.11.a | Information Location                     | Identify and document the location of CUI and the system components on which the information is processed and stored. | Functional     | Intersects With   | Statutory, Regulatory & Contractual Compliance                     | CPL-01   | Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.   | 3                        |   |
| 03.04.11.a | Information Location                     | Identify and document the location of CUI and the system components on which the information is processed and stored. | Functional     | Intersects With   | Compliance Scope   | CPL-01.2 | Mechanisms exist to document and validate the scope of security, compliance and resilience controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.   | 8                        |   |
| 03.04.11.a | Information Location                     | Identify and document the location of CUI and the system components on which the information is processed and stored. | Functional     | Intersects With   | Data & Asset Classification  | DCH-02   | Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.   | 8                        |   |
| 03.04.11.a | Information Location                     | Identify and document the location of CUI and the system components on which the information is processed and stored. | Functional     | Intersects With   | Sensitive Data Inventories   | DCH-06.2 | Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.  | 8                        |   |
| 03.04.11.a | Information Location                     | Identify and document the location of CUI and the system components on which the information is processed and stored. | Functional     | Intersects With   | Geographic Location of Data  | DCH-19   | Mechanisms exist to identify, document and maintain data flows for data that is resident (permanently or temporarily) within a person's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third parties.   | 3                        |   |
| 03.04.11.b | Information Location                     | Document changes to the system or system component location where CUI is processed and stored.                        | Functional     | Intersects With   | Data Action Mapping  | AST-02.8 | Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive/regulatory data is stored, transmitted or processed.   | 5                        |   |
| 03.04.11.b | Information Location                     | Document changes to the system or system component location where CUI is processed and stored.                        | Functional     | Intersects With   | Network Diagrams & Data Flow Diagrams (DFDs)                       | AST-04   | Mechanisms exist to maintain network architecture diagrams that:<br>(1) Contain sufficient detail to assess the security of the network's architecture;<br>(2) Reflect the current architecture of the network environment; and<br>(3) Document all sensitive/regulatory data flows.   | 3                        |   |
| 03.04.11.b | Information Location                     | Document changes to the system or system component location where CUI is processed and stored.                        | Functional     | Intersects With   | Asset Scope Classification   | AST-04.1 | Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).  | 3                        |   |
| 03.04.11.b | Information Location                     | Document changes to the system or system component location where CUI is processed and stored.                        | Functional     | Intersects With   | Control Applicability Boundary Graphical Representation            | AST-04.2 | Mechanisms exist to ensure control applicability is appropriately-determined for Technology Assets, Applications and/or Services (TAAS) and third parties by graphically representing applicable boundaries.   | 3                        |   |
| 03.04.11.b | Information Location                     | Document changes to the system or system component location where CUI is processed and stored.                        | Functional     | Intersects With   | Test, Validate & Document Changes                                  | CHG-02.2 | Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.   | 3                        |   |
| 03.04.11.b | Information Location                     | Document changes to the system or system component location where CUI is processed and stored.                        | Functional     | Intersects With   | Security Impact Analysis for Changes                               | CHG-03   | Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.  | 5                        |   |
| 03.04.11.b | Information Location                     | Document changes to the system or system component location where CUI is processed and stored.                        | 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.   | 8                        |   |
| 03.04.11.b | Information Location                     | Document changes to the system or system component location where CUI is processed and stored.                        | Functional     | Intersects With   | Sensitive Data Inventories   | DCH-06.2 | Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.  | 3                        |   |
| 03.04.11.b | Information Location                     | Document changes to the system or system component location where CUI is processed and stored.                        | Functional     | Intersects With   | Geographic Location of Data  | DCH-19   | Mechanisms exist to identify, document and maintain data flows for data that is resident (permanently or temporarily) within a person's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third parties.   | 3                        |   |
| 03.04.11.b | Information Location                     | Document changes to the system or system component location where CUI is processed and stored.                        | Functional     | Subset Of         | Applied Security, Compliance and Resilience Controls Documentation | IAO-03   | Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPOTDF) that are contained within the system;<br>(3) Describes the deficiency(ies);<br>(4) Risk associated with the deficiency(ies);<br>(5) Source deficiency identification/detection;<br>(6) Temporary compensating controls, if applicable;<br>(7) Points of Contact (POC) (e.g., asset/process owner). | 10                       |   |
| 03.04.11.b | Information Location                     | Document changes to the system or system component location where CUI is processed and stored.                        | Functional     | Intersects With   | Capabilities Deficiency Tracking                                   | IAO-05   | (2) Applicable security, compliance and/or resilience control;<br>(3) Description of the deficiency(ies);<br>(4) Risk associated with the deficiency(ies);<br>(5) Source deficiency identification/detection;<br>(6) Temporary compensating controls, if applicable;<br>(7) Points of Contact (POC) (e.g., asset/process owner).   | 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  |
|------------|--|--|----------------|-------------------|--|-----------|--|--------------------------|--|
| 03.04.12   | System and Component Configuration for High-Risk Areas | N/A  | Functional     | No Relationship   | N/A  | N/A       | N/A  | 0                        | No applicable SCF control  |
| 03.04.12.a | System and Component Configuration for High-Risk Areas | Issue systems or system components with the following configurations to individuals traveling to high-risk locations: [Assignment: organization-defined system configurations].                                  | Functional     | Subset Of         | Travel-Only Devices  | AST-24    | Mechanisms exist to issue personnel traveling overseas with temporary, loaner or "travel-only" end user technology (e.g., laptops and mobile devices) when traveling to authoritarian countries with a higher than average risk for Intellectual Property (IP) theft or espionage against individuals and private companies.   | 10                       | ODP Value: a configuration that has no CUI or FCI stored on the system and prevents the processing, storing, and transmission of CUI and FCI, unless a specific exception is granted in writing by the Contracting Officer.        |
| 03.04.12.a | System and Component Configuration for High-Risk Areas | Issue systems or system components with the following configurations to individuals traveling to high-risk locations: [Assignment: organization-defined system configurations].                                  | Functional     | Intersects With   | Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas                   | CFG-02.5  | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.  | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.04.12.a | System and Component Configuration for High-Risk Areas | Issue systems or system components with the following configurations to individuals traveling to high-risk locations: [Assignment: organization-defined system configurations].                                  | Functional     | Intersects With   | 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: <ul style="list-style-type: none"> <li>(1) Mission / business functions;</li> <li>(2) Operational environments;</li> <li>(3) Specific threats or vulnerabilities; or</li> <li>(4) Other conditions or situations that could affect mission / business success.</li> </ul> | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.04.12.b | System and Component Configuration for High-Risk Areas | Apply the following security requirements to the systems or components when the individuals return from travel: [Assignment: organization-defined security requirements].  | Functional     | Intersects With   | Travel-Only Devices  | AST-24    | Mechanisms exist to issue personnel traveling overseas with temporary, loaner or "travel-only" end user technology (e.g., laptops and mobile devices) when traveling to authoritarian countries with a higher than average risk for Intellectual Property (IP) theft or espionage against individuals and private companies.   | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.04.12.b | System and Component Configuration for High-Risk Areas | Apply the following security requirements to the systems or components when the individuals return from travel: [Assignment: organization-defined security requirements].  | Functional     | Intersects With   | Re-Imaging Devices After Travel  | AST-25    | Mechanisms exist to re-image end user technology (e.g., laptops and mobile devices) when returning from overseas travel to an authoritarian country with a higher than average risk for Intellectual Property (IP) theft or espionage against individuals and private companies.   | 8                        | ODP Value: examine the system for signs of physical tampering and take the appropriate actions, and then either purge and reimage all storage media or destroy the system  |
| 03.04.12.b | System and Component Configuration for High-Risk Areas | Apply the following security requirements to the systems or components when the individuals return from travel: [Assignment: organization-defined security requirements].  | Functional     | Intersects With   | Mobile Device Tampering  | MDM-04    | Mechanisms exist to protect mobile devices from tampering through inspecting devices returning from locations that the organization deems to be of significant risk, prior to the device being connected to the organization's network.  | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.05.01   | User Identification and Authentication                 | N/A  | Functional     | No Relationship   | N/A  | N/A       | N/A  | 0                        | No applicable SCF control  |
| 03.05.01.a | User Identification and Authentication                 | Uniquely identify and authenticate system users, and associate that unique identification with processes acting on behalf of those users.  | Functional     | Subset Of         | Identify & Access Management (IAM)   | IAC-01    | Mechanisms exist to facilitate the implementation of identification and access management controls.  | 10                       |  |
| 03.05.01.a | User Identification and Authentication                 | Uniquely identify and authenticate system users, and associate that unique identification with processes acting on behalf of those users.  | 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).   | 8                        |  |
| 03.05.01.a | User Identification and Authentication                 | Uniquely identify and authenticate system users, and associate that unique identification with processes acting on behalf of those users.  | Functional     | Intersects With   | 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.   | 8                        |  |
| 03.05.01.a | User Identification and Authentication                 | Uniquely identify and authenticate system users, and associate that unique identification with processes acting on behalf of those users.  | Functional     | Intersects With   | Identification & Authentication for Non-Organizational Users   | IAC-03    | Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.   | 8                        |  |
| 03.05.01.a | User Identification and Authentication                 | Uniquely identify and authenticate system users, and associate that unique identification with processes acting on behalf of those users.  | Functional     | Intersects With   | Identification & Authentication for Third-Party Technology Assets, Applications and/or Services (TAAS) | IAC-05    | Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).  | 3                        |  |
| 03.05.01.b | User Identification and Authentication                 | Re-authenticate users when [Assignment: organization-defined circumstances or situations requiring re-authentication].   | Functional     | Intersects With   | Re-Authentication  | IAC-14    | Mechanisms exist to force users and devices to re-authenticate according to organization-defined circumstances that necessitate re-authentication.   | 8                        | ODP Value: roles, authenticators, or credentials change (including modification of user privilege); when security categories of systems change; when the execution of privileged functions occurs; and after a session termination |
| 03.05.02   | Device Identification and Authentication               | Uniquely identify and authenticate [Assignment: organization-defined devices or types of devices] before establishing a system connection.   | 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).   | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.05.02   | Device Identification and Authentication               | Uniquely identify and authenticate [Assignment: organization-defined devices or types of devices] before establishing a system connection.   | Functional     | Intersects With   | Identification & Authentication for Devices  | IAC-04    | Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically based and replay resistant.  | 8                        | ODP Value: all devices for identification, where feasible for authentication, and document when not feasible   |
| 03.05.02   | Device Identification and Authentication               | Uniquely identify and authenticate [Assignment: organization-defined devices or types of devices] before establishing a system connection.   | Functional     | Intersects With   | Identification & Authentication for Third-Party Technology Assets, Applications and/or Services (TAAS) | IAC-05    | Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).  | 5                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.05.03   | Multi-Factor Authentication                            | Implement multi-factor authentication for access to privileged and non-privileged accounts.  | Functional     | Subset Of         | Multi-Factor Authentication (MFA)  | IAC-06    | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: <ul style="list-style-type: none"> <li>(1) Remote network access;</li> <li>(2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or</li> <li>(3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data.</li> </ul>  | 10                       |  |
| 03.05.03   | Multi-Factor Authentication                            | Implement multi-factor authentication for access to privileged and 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.  | 3                        |  |
| 03.05.03   | Multi-Factor Authentication                            | Implement multi-factor authentication for access to privileged and 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.  | 3                        |  |
| 03.05.03   | Multi-Factor Authentication                            | Implement multi-factor authentication for access to privileged and non-privileged accounts.  | Functional     | Intersects With   | Local Access to Privileged Accounts  | IAC-06.3  | Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.  | 3                        |  |
| 03.05.04   | Replay-Resistant Authentication                        | Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.   | Functional     | Equal             | Replay-Resistant Authentication  | IAC-02.2  | Automated mechanisms exist to employ replay-resistant authentication.  | 10                       |  |
| 03.05.05   | Identifier Management                                  | N/A  | Functional     | No Relationship   | N/A  | N/A       | N/A  | 0                        | No applicable SCF control  |
| 03.05.05.a | Identifier Management                                  | Receive authorization from organizational personnel or roles to assign an individual, group, role, service, or device identifier.  | Functional     | Subset Of         | Identify & Access Management (IAM)   | IAC-01    | Mechanisms exist to facilitate the implementation of identification and access management controls.  | 10                       |  |
| 03.05.05.a | Identifier Management                                  | Receive authorization from organizational personnel or roles to assign an individual, group, role, service, or device identifier.  | Functional     | Intersects With   | User Provisioning & De-Provisioning  | IAC-07    | Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.   | 8                        |  |
| 03.05.05.a | Identifier Management                                  | Receive authorization from organizational personnel or roles to assign an individual, group, role, service, or device identifier.  | Functional     | Intersects With   | Change of Roles & Duties   | IAC-07.1  | Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.  | 8                        |  |
| 03.05.05.a | Identifier Management                                  | Receive authorization from organizational personnel or roles to assign an individual, group, role, service, or device identifier.  | Functional     | Subset Of         | Management Approval For New or Changed Accounts  | IAC-28.1  | Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.  | 10                       |  |
| 03.05.05.b | Identifier Management                                  | Select and assign an identifier that identifies an individual, group, role, service, or device.  | Functional     | Intersects With   | Identifier Management (User Names)   | IAC-09    | Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).  | 5                        |  |
| 03.05.05.b | Identifier Management                                  | Select and assign an identifier that identifies an individual, group, role, service, or device.  | Functional     | Subset Of         | User Identity (ID) Management  | IAC-09.1  | Mechanisms exist to ensure proper user identification management for non-consumer users and administrators.  | 10                       |  |
| 03.05.05.b | Identifier Management                                  | Select and assign an identifier that identifies an individual, group, role, service, or device.  | 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).  | 3                        |  |
| 03.05.05.c | Identifier Management                                  | Prevent the reuse of identifiers for [Assignment: organization-defined time period].   | Functional     | Intersects With   | Identifier Management (User Names)   | IAC-09    | Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).  | 8                        | ODP Value: at least ten (10) years   |
| 03.05.05.c | Identifier Management                                  | Prevent the reuse of identifiers for [Assignment: organization-defined time period].   | 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                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.05.05.d | Identifier Management                                  | Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].  | Functional     | Subset Of         | 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).   | 10                       | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.05.05.d | Identifier Management                                  | Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].  | Functional     | Intersects With   | 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.   | 8                        | ODP Value: privileged or non-privileged users; contractors, foreign nationals, and/or non-organizational users   |
| 03.05.05.d | Identifier Management                                  | Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].  | Functional     | Intersects With   | Identifier Management (User Names)   | IAC-09    | Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).  | 3                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.05.05.d | Identifier Management                                  | Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].  | Functional     | Intersects With   | Identify User Status   | IAC-09.2  | Mechanisms exist to identify contractors and other third-party users through unique username characteristics.  | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.05.05.d | Identifier Management                                  | Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].  | Functional     | Intersects With   | Privileged Account Identifiers   | IAC-09.5  | Mechanisms exist to uniquely manage privileged accounts to identify the account as a privileged user or service.   | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.05.05.d | Identifier Management                                  | Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].  | 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                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.05.06   | Identifier Management                                  | Consistency with SP 800-53.  | Functional     | No Relationship   | N/A  | N/A       | N/A  | 0                        | No applicable SCF control  |
| 03.05.07   | Password Management                                    | N/A  | Functional     | No Relationship   | N/A  | N/A       | N/A  | 0                        | No applicable SCF control  |
| 03.05.07.a | Password Management                                    | Maintain a list of commonly-used, expected, or compromised passwords, and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised. | 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).   | 3                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.05.07.a | Password Management                                    | Maintain a list of commonly-used, expected, or compromised passwords, and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised. | Functional     | Intersects With   | Authenticator Management   | IAC-10    | Mechanisms exist to: <ul style="list-style-type: none"> <li>(1) Securely manage authenticators for users and devices; and</li> <li>(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.</li> </ul>   | 3                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.05.07.a | Password Management                                    | Maintain a list of commonly-used, expected, or compromised passwords, and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised. | Functional     | Intersects With   | Password Managers  | IAC-10.11 | Mechanisms exist to protect and store passwords via a password manager tool.   | 8                        | ODP Value: at least quarterly  |
| 03.05.07.a | Password Management                                    | Maintain a list of commonly-used, expected, or compromised passwords, and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised. | Functional     | Intersects With   | Automated Support For Password Strength  | IAC-10.4  | Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.   | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.05.07.b | Password Management                                    | Verify that passwords are not found on the list of commonly used, expected, or compromised passwords when users create or update passwords.  | 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).   | 3                        |  |
| 03.05.07.b | Password Management                                    | Verify that passwords are not found on the list of commonly used, expected, or compromised passwords when users create or update passwords.  | Functional     | Intersects With   | Authenticator Management   | IAC-10    | Mechanisms exist to: <ul style="list-style-type: none"> <li>(1) Securely manage authenticators for users and devices; and</li> <li>(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.</li> </ul>   | 3                        |  |
| 03.05.07.b | Password Management                                    | Verify that passwords are not found on the list of commonly used, expected, or compromised passwords when users create or update passwords.  | Functional     | Intersects With   | Password Managers  | IAC-10.11 | Mechanisms exist to protect and store passwords via a password manager tool.   | 8                        |  |
| 03.05.07.b | Password Management                                    | Verify that passwords are not found on the list of commonly used, expected, or compromised passwords when users create or update passwords.  | Functional     | Intersects With   | Automated Support For Password Strength  | IAC-10.4  | Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.   | 8                        |  |
| 03.05.07.c | Password Management                                    | Transmit passwords only over cryptographically protected channels.   | 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).   | 3                        |  |

| 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  |
|------------|--------------------------|--|----------------|-------------------|--|-----------|---|--------------------------|--|
| 03.05.07.c | Password Management      | Transmit passwords only over cryptographically protected channels.   | Functional     | Intersects With   | Authenticator Management                                 | IAc-10    | Mechanisms exist to:<br>(1) Securely manage authenticators for users and devices; and<br>(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.                 | 3                        |  |
| 03.05.07.c | Password Management      | Transmit passwords only over cryptographically protected channels.   | Functional     | Intersects With   | Password Managers  | IAc-10.11 | Mechanisms exist to protect and store passwords via a password manager tool.  | 3                        |  |
| 03.05.07.c | Password Management      | Transmit passwords only over cryptographically protected channels.   | Functional     | Subset Of         | Protection of Authenticators                             | IAc-10.5  | Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.   | 10                       |  |
| 03.05.07.c | Password Management      | Transmit passwords only over cryptographically protected channels.   | 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).   | 8                        |  |
| 03.05.07.d | Password Management      | Store passwords in a cryptographically protected form.   | 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                        |  |
| 03.05.07.d | Password Management      | Store passwords in a cryptographically protected form.   | 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).  | 8                        |  |
| 03.05.07.d | Password Management      | Store passwords in a cryptographically protected form.   | Functional     | Intersects With   | Authenticator Management                                 | IAc-10    | Mechanisms exist to:<br>(1) Securely manage authenticators for users and devices; and<br>(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.                 | 5                        |  |
| 03.05.07.d | Password Management      | Store passwords in a cryptographically protected form.   | Functional     | Intersects With   | Password Managers  | IAc-10.11 | Mechanisms exist to protect and store passwords via a password manager tool.  | 8                        |  |
| 03.05.07.d | Password Management      | Store passwords in a cryptographically protected form.   | Functional     | Intersects With   | Protection of Authenticators                             | IAc-10.5  | Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.   | 8                        |  |
| 03.05.07.d | Password Management      | Store passwords in a cryptographically protected form.   | Functional     | Intersects With   | No Embedded Unencrypted Static Authenticators            | IAc-10.6  | Mechanisms exist to ensure that unencrypted, static authenticators are not embedded in applications, scripts or stored on function keys.  | 8                        |  |
| 03.05.07.d | Password Management      | Store passwords in a cryptographically protected form.   | 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).   | 8                        |  |
| 03.05.07.e | Password Management      | Select a new password upon first use after account recovery.   | 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. | 8                        |  |
| 03.05.07.e | Password Management      | Select a new password upon first use after account recovery.   | 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).  | 8                        |  |
| 03.05.07.e | Password Management      | Select a new password upon first use after account recovery.   | Functional     | Intersects With   | Authenticator Management                                 | IAc-10    | Mechanisms exist to:<br>(1) Securely manage authenticators for users and devices; and<br>(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.                 | 8                        |  |
| 03.05.07.e | Password Management      | Select a new password upon first use after account recovery.   | Functional     | Subset Of         | Password-Based Authentication                            | IAc-10.1  | Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.   | 10                       |  |
| 03.05.07.e | Password Management      | Select a new password upon first use after account recovery.   | Functional     | Intersects With   | Default Authenticators                                   | IAc-10.8  | Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.   | 3                        |  |
| 03.05.07.e | Password Management      | Select a new password upon first use after account recovery.   | 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                        |  |
| 03.05.07.f | Password Management      | Enforce the following composition and complexity rules for passwords: [Assignment: organization-defined composition and complexity rules]  | 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                       | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.05.07.f | Password Management      | Enforce the following composition and complexity rules for passwords: [Assignment: organization-defined composition and complexity rules]  | Functional     | Intersects With   | Authenticator Management                                 | IAc-10    | Mechanisms exist to:<br>(1) Securely manage authenticators for users and devices; and<br>(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.                 | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.05.07.f | Password Management      | Enforce the following composition and complexity rules for passwords: [Assignment: organization-defined composition and complexity rules]  | Functional     | Intersects With   | Password-Based Authentication                            | IAc-10.1  | Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.   | 8                        | ODP Values:<br>(1) Must have a minimum length of 16 characters.<br>(2) Contains a string of characters that does not include the user's account name or full name.   |
| 03.05.07.f | Password Management      | Enforce the following composition and complexity rules for passwords: [Assignment: organization-defined composition and complexity rules]  | Functional     | Intersects With   | Password Managers  | IAc-10.11 | Mechanisms exist to protect and store passwords via a password manager tool.  | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.05.07.f | Password Management      | Enforce the following composition and complexity rules for passwords: [Assignment: organization-defined composition and complexity rules]  | 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).   | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.05.08   | Password Management      | Consistency with SP 800-53.  | Functional     | No Relationship   | N/A  | N/A       | N/A   | 0                        | No applicable SCF control  |
| 03.05.09   | Password Management      | Consistency with SP 800-53.  | Functional     | No Relationship   | N/A  | N/A       | N/A   | 0                        | No applicable SCF control  |
| 03.05.10   | Withdrawn                | Incorporated into 03.05.07.  | Functional     | No Relationship   | N/A  | N/A       | N/A   | 0                        | No applicable SCF control  |
| 03.05.11   | Authentication Feedback  | Obscure feedback of authentication information during the authentication process.  | Functional     | Equal             | Authenticator Feedback                                   | IAc-11    | Mechanisms exist to obscure the feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.                     | 10                       |  |
| 03.05.12   | Authenticator Management | N/A  | Functional     | No Relationship   | N/A  | N/A       | N/A   | 0                        | No applicable SCF control  |
| 03.05.12.a | Authenticator Management | Verify the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution.                                  | Functional     | Subset Of         | Authenticator Management                                 | IAc-10    | Mechanisms exist to:<br>(1) Securely manage authenticators for users and devices; and<br>(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.                 | 10                       |  |
| 03.05.12.a | Authenticator Management | Verify the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution.                                  | Functional     | Intersects With   | In-Person or Trusted Third-Party Registration            | IAc-10.3  | Mechanisms exist to conduct in-person or trusted third-party identity verification before user accounts for third-parties are created.  | 8                        |  |
| 03.05.12.a | Authenticator Management | Verify the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution.                                  | Functional     | Intersects With   | Identity Proofing (Identity Verification)                | IAc-28    | Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions.  | 8                        |  |
| 03.05.12.b | Authenticator Management | Establish initial authenticator content for any authenticators issued by the organization.   | Functional     | Subset Of         | Authenticator Management                                 | IAc-10    | Mechanisms exist to:<br>(1) Securely manage authenticators for users and devices; and<br>(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.                 | 10                       |  |
| 03.05.12.b | Authenticator Management | Establish initial authenticator content for any authenticators issued by the organization.   | Functional     | Intersects With   | Password-Based Authentication                            | IAc-10.1  | Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.   | 5                        |  |
| 03.05.12.c | Authenticator Management | Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.           | Functional     | Subset Of         | Authenticator Management                                 | IAc-10    | Mechanisms exist to:<br>(1) Securely manage authenticators for users and devices; and<br>(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.                 | 10                       |  |
| 03.05.12.c | Authenticator Management | Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.           | Functional     | Intersects With   | Password-Based Authentication                            | IAc-10.1  | Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.   | 5                        |  |
| 03.05.12.c | Authenticator Management | Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.           | Functional     | Intersects With   | Identity Proofing (Identity Verification)                | IAc-28    | Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions.  | 5                        |  |
| 03.05.12.d | Authenticator Management | Change default authenticators at first use.  | 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                       |  |
| 03.05.12.d | Authenticator Management | Change default authenticators at first use.  | 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).  | 8                        |  |
| 03.05.12.d | Authenticator Management | Change default authenticators at first use.  | Functional     | Intersects With   | Authenticator Management                                 | IAc-10    | Mechanisms exist to:<br>(1) Securely manage authenticators for users and devices; and<br>(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.                 | 8                        |  |
| 03.05.12.d | Authenticator Management | Change default authenticators at first use.  | Functional     | Intersects With   | Password-Based Authentication                            | IAc-10.1  | Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.   | 8                        |  |
| 03.05.12.d | Authenticator Management | Change default authenticators at first use.  | Functional     | Intersects With   | Default Authenticators                                   | IAc-10.8  | Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.   | 8                        |  |
| 03.05.12.d | Authenticator Management | Change default authenticators at first use.  | 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).   | 8                        |  |
| 03.05.12.e | Authenticator Management | Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].                           | Functional     | Subset Of         | Identity & Access Management (IAM)                       | IAc-01    | Mechanisms exist to facilitate the implementation of identification and access management controls.   | 10                       | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.05.12.e | Authenticator Management | Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].                           | Functional     | Intersects With   | Authenticator Management                                 | IAc-10    | Mechanisms exist to:<br>(1) Securely manage authenticators for users and devices; and<br>(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.                 | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.05.12.e | Authenticator Management | Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].                           | Functional     | Intersects With   | Password-Based Authentication                            | IAc-10.1  | Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.   | 8                        | ODP Values:<br>(1) never for passwords where MFA is employed, at least every five (5) years for hard tokens and identification badges, and at least every three (3) years for all other authenticators.<br>(2) after a relevant security incident or any evidence of compromise or loss. |
| 03.05.12.e | Authenticator Management | Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].                           | 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                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.05.12.f | Authenticator Management | Protect authenticator content from unauthorized disclosure and modification.   | 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).  | 3                        |  |
| 03.05.12.f | Authenticator Management | Protect authenticator content from unauthorized disclosure and modification.   | Functional     | Intersects With   | Authenticator Management                                 | IAc-10    | Mechanisms exist to:<br>(1) Securely manage authenticators for users and devices; and<br>(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.                 | 5                        |  |
| 03.05.12.f | Authenticator Management | Protect authenticator content from unauthorized disclosure and modification.   | Functional     | Intersects With   | Password-Based Authentication                            | IAc-10.1  | Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.   | 3                        |  |
| 03.05.12.f | Authenticator Management | Protect authenticator content from unauthorized disclosure and modification.   | Functional     | Subset Of         | Protection of Authenticators                             | IAc-10.5  | Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.   | 10                       |  |
| 03.05.12.f | Authenticator Management | Protect authenticator content from unauthorized disclosure and modification.   | 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).   | 3                        |  |
| 03.06.01   | Incident Handling        | Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery. | 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                       |  |

| 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  |
|---------------|---|--|----------------|-------------------|---|----------|---|--------------------------|--|
| 03.06.01      | Incident Handling                                       | Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery. | Functional     | Intersects With   | Incident Handling   | IRO-02   | Mechanisms exist to cover:<br>1) Preparation;<br>2) Automated event detection or manual incident report intake;<br>3) Analysis;<br>4) Containment;<br>5) Eradication; and<br>6) Recovery.   | 8                        |  |
| 03.06.01      | Incident Handling                                       | Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery. | Functional     | Intersects With   | Incident Response Plan (IRP)  | IRO-04   | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.  | 8                        |  |
| 03.06.01      | Incident Handling                                       | Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery. | Functional     | Intersects With   | Sensitive / Regulated Data Spill Response   | IRO-12   | Mechanisms exist to respond to sensitive/regulated data spills.   | 3                        |  |
| 03.06.02      | Incident Monitoring, Reporting, and Response Assistance | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.06.02.a    | Incident Monitoring, Reporting, and Response Assistance | Track and document system security incidents.  | Functional     | Subset Of         | Incident Handling   | IRO-02   | Mechanisms exist to cover:<br>1) Preparation;<br>2) Automated event detection or manual incident report intake;<br>3) Analysis;<br>4) Containment;<br>5) Eradication; and<br>6) Recovery.   | 10                       |  |
| 03.06.02.a    | Incident Monitoring, Reporting, and Response Assistance | Track and document system security incidents.  | Functional     | Intersects With   | 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.   | 8                        |  |
| 03.06.02.b    | Incident Monitoring, Reporting, and Response Assistance | Report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period].   | Functional     | Subset Of         | Incident Handling   | IRO-02   | Mechanisms exist to cover:<br>1) Preparation;<br>2) Automated event detection or manual incident report intake;<br>3) Analysis;<br>4) Containment;<br>5) Eradication; and<br>6) Recovery.   | 10                       | ODP Value: near real time or as soon as practicable upon discovery   |
| 03.06.02.b    | Incident Monitoring, Reporting, and Response Assistance | Report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period].   | Functional     | Intersects With   | 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.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.06.02.b    | Incident Monitoring, Reporting, and Response Assistance | Report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period].   | Functional     | Intersects With   | Incident Stakeholder Reporting  | IRO-10   | Mechanisms exist to timely-report incidents to applicable:<br>1) Internal stakeholders;<br>2) Affected clients & third parties; and<br>3) Regulatory authorities.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.06.02.b    | Incident Monitoring, Reporting, and Response Assistance | Report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period].   | Functional     | Intersects With   | Cyber Incident Reporting for Sensitive / Regulated Data                               | IRO-10.2 | Mechanisms exist to report sensitive/regulated data incidents in a timely manner.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.06.02.c    | Incident Monitoring, Reporting, and Response Assistance | Report incident information to [Assignment: organization-defined authorities].   | Functional     | Subset Of         | Incident Handling   | IRO-02   | Mechanisms exist to cover:<br>1) Preparation;<br>2) Automated event detection or manual incident report intake;<br>3) Analysis;<br>4) Containment;<br>5) Eradication; and<br>6) Recovery.   | 10                       | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.06.02.c    | Incident Monitoring, Reporting, and Response Assistance | Report incident information to [Assignment: organization-defined authorities].   | Functional     | Intersects With   | Incident Stakeholder Reporting  | IRO-10   | Mechanisms exist to timely-report incidents to applicable:<br>1) Internal stakeholders;<br>2) Affected clients & third parties; and<br>3) Regulatory authorities.   | 8                        | ODP Value: all applicable personnel and entities as specified by the contract, and in accordance with any incident response plan notification procedures |
| 03.06.02.c    | Incident Monitoring, Reporting, and Response Assistance | Report incident information to [Assignment: organization-defined authorities].   | Functional     | Intersects With   | Cyber Incident Reporting for Sensitive / Regulated Data                               | IRO-10.2 | Mechanisms exist to report sensitive/regulated data incidents in a timely manner.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.06.02.c    | Incident Monitoring, Reporting, and Response Assistance | Report incident information to [Assignment: organization-defined authorities].   | Functional     | Intersects With   | Regulatory & Law Enforcement Contacts   | IRO-14   | Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.  | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.06.02.d    | Incident Monitoring, Reporting, and Response Assistance | Provide an incident response support resource that offers advice and assistance to system users on handling and reporting incidents.   | Functional     | Subset Of         | Incident Handling   | IRO-02   | Mechanisms exist to cover:<br>1) Preparation;<br>2) Automated event detection or manual incident report intake;<br>3) Analysis;<br>4) Containment;<br>5) Eradication; and<br>6) Recovery.   | 10                       |  |
| 03.06.02.d    | Incident Monitoring, Reporting, and Response Assistance | Provide an incident response support resource that offers advice and assistance to system users on handling and reporting 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                       |  |
| 03.06.03      | Incident Response Testing                               | Test the effectiveness of the incident response capability [Assignment: organization-defined frequency].   | 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                       | ODP Value: at least every 12 months  |
| 03.06.04      | Incident Response Training                              | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.06.04.a    | Incident Response Training                              | Provide incident response training to system users consistent with assigned roles and responsibilities.  | Functional     | Intersects With   | Defined Roles & Responsibilities  | HRS-03   | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.  | 8                        |  |
| 03.06.04.a    | Incident Response Training                              | Provide incident response training to system users consistent with assigned roles and responsibilities.  | Functional     | Intersects With   | Formal Indocination   | HRS-04.2 | Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access.   | 8                        |  |
| 03.06.04.a    | Incident Response Training                              | Provide incident response training to system users consistent with assigned roles and responsibilities.  | Functional     | Subset Of         | Incident Response Training  | IRO-05   | Mechanisms exist to train personnel in their incident response roles and responsibilities.  | 10                       |  |
| 03.06.04.a    | Incident Response Training                              | Provide incident response training to system users consistent with assigned 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:<br>1) Before authorizing access to the system or performing assigned duties;<br>2) When required by system changes; and<br>3) Annually thereafter.   | 8                        |  |
| 03.06.04.a.01 | Incident Response Training                              | Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access.  | Functional     | Intersects With   | Formal Indocination   | HRS-04.2 | Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access.   | 3                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.06.04.a.01 | Incident Response Training                              | Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access.  | Functional     | Intersects With   | Role-Based Security, Compliance & Resilience Training                                 | SAT-03   | Mechanisms exist to provide role-based security, compliance and resilience-related training:<br>1) Before authorizing access to the system or performing assigned duties;<br>2) When required by system changes; and<br>3) Annually thereafter.   | 8                        | ODP Value: ten (10) days for privileged users, thirty (30) days for all other roles  |
| 03.06.04.a.02 | Incident Response Training                              | When required by system changes, and   | Functional     | Intersects With   | Role-Based Security, Compliance & Resilience Training                                 | SAT-03   | Mechanisms exist to provide role-based security, compliance and resilience-related training:<br>1) Before authorizing access to the system or performing assigned duties;<br>2) When required by system changes; and<br>3) Annually thereafter.   | 5                        |  |
| 03.06.04.a.02 | Incident Response Training                              | When required by system changes, and   | Functional     | Intersects With   | Cyber Threat Environment  | SAT-03.6 | Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.   | 5                        |  |
| 03.06.04.a.03 | Incident Response Training                              | [Assignment: organization-defined frequency] thereafter.   | Functional     | Intersects With   | Incident Response Training  | IRO-05   | Mechanisms exist to train personnel in their incident response roles and responsibilities.  | 8                        | ODP Value: at least every 12 months  |
| 03.06.04.a.03 | Incident Response Training                              | [Assignment: organization-defined frequency] thereafter.   | Functional     | Intersects With   | 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 to their job function.  | 8                        | ODP Value: at least every 12 months  |
| 03.06.04.b    | Incident Response Training                              | Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].                             | Functional     | Intersects With   | IRP Update  | IRO-04.2 | Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.   | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.06.04.b    | Incident Response Training                              | Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].                             | Functional     | Intersects With   | Continuous Incident Response Improvements   | IRO-04.3 | Mechanisms exist to use qualitative and quantitative data from incident response testing to:<br>1) Determine the effectiveness of incident response processes;<br>2) Continuously improve incident response processes; and<br>3) Provide incident response measures and metrics that are accurate, consistent and in a reproducible format. | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.06.04.b    | Incident Response Training                              | Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].                             | Functional     | Intersects With   | Root Cause Analysis (RCA) & Lessons Learned   | IRO-13   | Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.  | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.06.04.b    | Incident Response Training                              | Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].                             | Functional     | Intersects With   | Role-Based Security, Compliance & Resilience Training                                 | SAT-03   | Mechanisms exist to provide role-based security, compliance and resilience-related training:<br>1) Before authorizing access to the system or performing assigned duties;<br>2) When required by system changes; and<br>3) Annually thereafter.   | 8                        | ODP Values:<br>1) at least every 12 months<br>2) significant, novel incidents, or significant changes to risks   |
| 03.06.04.b    | Incident Response Training                              | Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].                             | Functional     | Intersects With   | Continuing Professional Education (CPE) - Security, Compliance & Resilience Personnel | SAT-03.7 | Mechanisms exist to ensure security, compliance and resilience personnel receive Continuing Professional Education (CPE) training to maintain currency and proficiency with industry-recognized secure practices that are pertinent to their assigned roles and responsibilities.   | 3                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.06.05      | Incident Response Plan                                  | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.06.05.a    | Incident Response Plan                                  | Develop 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                       |  |
| 03.06.05.a.01 | Incident Response Plan                                  | Provides the organization with a roadmap for implementing its 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                       |  |
| 03.06.05.a.02 | 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                       |  |
| 03.06.05.a.03 | 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                       |  |
| 03.06.05.a.04 | Incident Response Plan                                  | Defines reportable 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                       |  |
| 03.06.05.a.05 | Incident Response Plan                                  | Addresses the sharing of incident information, 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                       |  |
| 03.06.05.a.06 | Incident Response Plan                                  | Designates responsibilities to organizational entities, personnel, or roles.   | 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                       |  |
| 03.06.05.b    | Incident Response Plan                                  | Distribute copies of the incident response plan to designated incident response personnel (identified by name and/or by role) and organizational elements.                             | 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                       |  |
| 03.06.05.c    | Incident Response Plan                                  | Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing.                              | 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                        |  |
| 03.06.05.d    | Incident Response Plan                                  | Protect the incident response plan from unauthorized disclosure.   | Functional     | Subset Of         | Sensitive / Regulated Data Protection   | DCH-01.2 | Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.  | 10                       |  |
| 03.06.05.d    | Incident Response Plan                                  | Protect the incident response plan from unauthorized disclosure.   | Functional     | Intersects With   | Defined Roles & Responsibilities  | HRS-03   | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.  | 8                        |  |
| 03.06.05.d    | Incident Response Plan                                  | Protect the incident response plan from unauthorized disclosure.   | Functional     | Intersects With   | 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.  | 8                        |  |

| 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                     |
|------------|------------------------|--|----------------|-------------------|--|----------|---|--------------------------|---------------------------|
| 03.06.05.d | Incident Response Plan | Protect the incident response plan from unauthorized disclosure.   | Functional     | Intersects With   | Access To Sensitive / Regulated Data                                     | IAC-20.1 | Mechanisms exist to limit access to sensitive/regulated data to only those individuals whose job requires such access.  | 8                        |                           |
| 03.07.01   | Withdrawn              | Recategorized as NCO.  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control |
| 03.07.02   | Withdrawn              | Incorporated into 03.07.04 and 03.07.06.   | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control |
| 03.07.03   | Withdrawn              | Incorporated into 03.08.03.  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control |
| 03.07.04   | Maintenance Tools      | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control |
| 03.07.04.a | Maintenance Tools      | Approve, control, and monitor the use of system maintenance tools.   | 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                        |                           |
| 03.07.04.a | Maintenance Tools      | Approve, control, and monitor the use of system maintenance tools.   | Functional     | Intersects With   | Security of Assets & Media   | AST-05   | Mechanisms exist to maintain strict control over the internal or external distribution of any kind of sensitive/regulated media.  | 3                        |                           |
| 03.07.04.a | Maintenance Tools      | Approve, control, and monitor the use of system maintenance tools.   | 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                       |                           |
| 03.07.04.a | Maintenance Tools      | Approve, control, and monitor the use of system maintenance tools.   | Functional     | Intersects With   | Controlled Maintenance   | MNT-02   | Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).  | 8                        |                           |
| 03.07.04.a | Maintenance Tools      | Approve, control, and monitor the use of system maintenance tools.   | Functional     | Intersects With   | 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).  | 8                        |                           |
| 03.07.04.a | Maintenance Tools      | Approve, control, and monitor the use of system maintenance tools.   | Functional     | Intersects With   | Preventative Maintenance   | MNT-03.1 | Mechanisms exist to perform preventive maintenance on critical Technology Assets, Applications and/or Services (TAAS).  | 8                        |                           |
| 03.07.04.a | Maintenance Tools      | Approve, control, and monitor the use of system maintenance tools.   | Functional     | Intersects With   | Maintenance Tools  | MNT-04   | Mechanisms exist to control and monitor the use of system maintenance tools.  | 8                        |                           |
| 03.07.04.a | Maintenance Tools      | Approve, control, and monitor the use of system maintenance tools.   | Functional     | Intersects With   | Off-Site Maintenance   | MNT-09   | Mechanisms exist to ensure off-site maintenance activities are conducted securely and the assets/IT undergoing maintenance actions are secured during physical transfer and storage while off-site.   | 3                        |                           |
| 03.07.04.b | Maintenance Tools      | Check media with diagnostic and test programs for malicious code before it is used in the system.  | 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                       |                           |
| 03.07.04.c | Maintenance Tools      | Prevent the removal of system maintenance equipment containing CUI by verifying that there is no CUI on the equipment, sanitizing or destroying the equipment, or retaining the equipment within the facility. | Functional     | Intersects With   | Secure Disposal / Destruction or Re-Use of Equipment                     | AST-09   | Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.   | 5                        |                           |
| 03.07.04.c | Maintenance Tools      | Prevent the removal of system maintenance equipment containing CUI by verifying that there is no CUI on the equipment, sanitizing or destroying the equipment, or retaining the equipment within the facility. | Functional     | Intersects With   | System Media Sanitization  | DCH-09   | Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.   | 8                        |                           |
| 03.07.04.c | Maintenance Tools      | Prevent the removal of system maintenance equipment containing CUI by verifying that there is no CUI on the equipment, sanitizing or destroying the equipment, or retaining the equipment within the facility. | Functional     | Intersects With   | Prevent Unauthorized Removal   | MNT-04.3 | Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational information.  | 8                        |                           |
| 03.07.05   | Nonlocal Maintenance   | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control |
| 03.07.05.a | Nonlocal Maintenance   | Approve and monitor nonlocal maintenance and diagnostic activities.  | 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).  | 8                        |                           |
| 03.07.05.a | Nonlocal Maintenance   | Approve and monitor nonlocal maintenance and diagnostic activities.  | Functional     | Intersects With   | Privileged Access by Non-Organizational Users                            | IAC-05.2 | Mechanisms exist to prohibit privileged access by non-organizational users.   | 3                        |                           |
| 03.07.05.a | Nonlocal Maintenance   | Approve and monitor nonlocal maintenance and diagnostic activities.  | Functional     | Intersects With   | Controlled Maintenance   | MNT-02   | Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).  | 8                        |                           |
| 03.07.05.a | Nonlocal Maintenance   | Approve and monitor nonlocal maintenance and diagnostic activities.  | Functional     | Intersects With   | Remote Maintenance   | MNT-05   | Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.   | 8                        |                           |
| 03.07.05.a | Nonlocal Maintenance   | Approve and monitor nonlocal maintenance and diagnostic activities.  | 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.   | 3                        |                           |
| 03.07.05.a | Nonlocal Maintenance   | Approve and monitor nonlocal maintenance and diagnostic activities.  | Functional     | Intersects With   | Remote Maintenance Pre-Approval  | MNT-05.5 | Mechanisms exist to require maintenance personnel to obtain pre-approval and scheduling for remote, non-local maintenance sessions.   | 8                        |                           |
| 03.07.05.b | Nonlocal Maintenance   | Implement multi-factor authentication and replay resistance in the establishment of nonlocal maintenance and diagnostic sessions.  | Functional     | Intersects With   | Replay-Resistant Authentication  | IAC-02.2 | Automated mechanisms exist to employ replay-resistant authentication.   | 8                        |                           |
| 03.07.05.b | Nonlocal Maintenance   | Implement multi-factor authentication and replay resistance in the establishment of nonlocal maintenance and diagnostic sessions.  | Functional     | Intersects With   | Multi-Factor Authentication (MFA)  | IAC-06   | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.    | 8                        |                           |
| 03.07.05.b | Nonlocal Maintenance   | Implement multi-factor authentication and replay resistance in the establishment of nonlocal maintenance and diagnostic sessions.  | Functional     | Intersects With   | Remote Maintenance   | MNT-05   | Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.   | 5                        |                           |
| 03.07.05.b | Nonlocal Maintenance   | Implement multi-factor authentication and replay resistance in the establishment of nonlocal maintenance and diagnostic sessions.  | Functional     | Intersects With   | Remote Maintenance Cryptographic Protection                              | MNT-05.3 | Cryptographic mechanisms exist to protect the integrity and confidentiality of remote, non-local maintenance and diagnostic communications.   | 3                        |                           |
| 03.07.05.c | Nonlocal Maintenance   | Terminate session and network connections when nonlocal maintenance is completed.  | Functional     | Intersects With   | 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.  | 3                        |                           |
| 03.07.05.c | Nonlocal Maintenance   | Terminate session and network connections when nonlocal maintenance is completed.  | Functional     | Intersects With   | Remote Maintenance   | MNT-05   | Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.   | 5                        |                           |
| 03.07.05.c | Nonlocal Maintenance   | Terminate session and network connections when nonlocal maintenance is completed.  | Functional     | Intersects With   | Remote Maintenance Disconnect Verification                               | MNT-05.4 | Mechanisms exist to provide remote disconnect verification to ensure remote, non-local maintenance and diagnostic sessions are properly terminated.   | 8                        |                           |
| 03.07.06   | Maintenance Personnel  | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control |
| 03.07.06.a | Maintenance Personnel  | Establish a process for maintenance personnel authorization.   | Functional     | Intersects With   | Defined Roles & Responsibilities   | HRS-03   | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.  | 5                        |                           |
| 03.07.06.a | Maintenance Personnel  | Establish a process for maintenance personnel authorization.   | Functional     | Intersects With   | Role-Based Access Control (RBAC)   | IAC-08   | Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAAS) to restrict access to individuals assigned specific roles with legitimate business needs.   | 5                        |                           |
| 03.07.06.a | Maintenance Personnel  | Establish a process for maintenance personnel authorization.   | 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                       |                           |
| 03.07.06.a | Maintenance Personnel  | Establish a process for maintenance personnel authorization.   | Functional     | Intersects With   | Authorized Maintenance Personnel   | MNT-06   | Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.   | 5                        |                           |
| 03.07.06.a | Maintenance Personnel  | Establish a process for maintenance personnel authorization.   | Functional     | Intersects With   | Maintenance Personnel Without Appropriate Access                         | MNT-06.1 | Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.  | 5                        |                           |
| 03.07.06.a | Maintenance Personnel  | Establish a process for maintenance personnel authorization.   | Functional     | Intersects With   | Non-System Related Maintenance   | MNT-06.2 | Mechanisms exist to ensure that non-escorted personnel performing non-IT maintenance activities in the physical proximity of systems have required access authorizations.   | 5                        |                           |
| 03.07.06.a | Maintenance Personnel  | Establish a process for maintenance personnel authorization.   | Functional     | Intersects With   | Third-Party Management   | TPM-01   | Mechanisms exist to facilitate the implementation of third-party management controls.   | 5                        |                           |
| 03.07.06.a | Maintenance Personnel  | Establish a process for maintenance personnel authorization.   | Functional     | Intersects With   | Third-Party Inventories  | TPM-01.1 | Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).      | 5                        |                           |
| 03.07.06.a | Maintenance Personnel  | Establish a process for maintenance personnel authorization.   | Functional     | Intersects With   | 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).                                      | 5                        |                           |
| 03.07.06.a | Maintenance Personnel  | Establish a process for maintenance personnel authorization.   | Functional     | Intersects With   | Responsible, Accountable, Supportive, Consulted & Informed (RASC) Matrix | TPM-05.4 | Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASC) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).   | 3                        |                           |
| 03.07.06.b | Maintenance Personnel  | Maintain a list of authorized maintenance organizations or personnel.  | Functional     | Equal             | Authorized Maintenance Personnel   | MNT-06   | Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.   | 10                       |                           |
| 03.07.06.c | Maintenance Personnel  | Verify that non-escorted personnel who perform maintenance on the system possess the required access authorizations.   | Functional     | Intersects With   | Authorized Maintenance Personnel   | MNT-06   | Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.   | 5                        |                           |
| 03.07.06.c | Maintenance Personnel  | Verify that non-escorted personnel who perform maintenance on the system possess the required access authorizations.   | Functional     | Subset Of         | Maintenance Personnel Without Appropriate Access                         | MNT-06.1 | Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.  | 10                       |                           |
| 03.07.06.c | Maintenance Personnel  | Verify that non-escorted personnel who perform maintenance on the system possess the required access authorizations.   | Functional     | Intersects With   | Non-System Related Maintenance   | MNT-06.2 | Mechanisms exist to ensure that non-escorted personnel performing non-IT maintenance activities in the physical proximity of systems have required access authorizations.   | 5                        |                           |
| 03.07.06.d | Maintenance Personnel  | Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.    | Functional     | 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.   | 8                        |                           |
| 03.07.06.d | Maintenance Personnel  | Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.    | Functional     | Intersects With   | Authorized Maintenance Personnel   | MNT-06   | Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.   | 8                        |                           |
| 03.07.06.d | Maintenance Personnel  | Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.    | Functional     | Intersects With   | Maintenance Personnel Without Appropriate Access                         | MNT-06.1 | Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.  | 8                        |                           |
| 03.08.01   | Media Storage          | Physically control and securely store system media that contain CUI.   | Functional     | Subset Of         | Data Protection  | DCH-01   | Mechanisms exist to facilitate the implementation of data protection controls.  | 10                       |                           |
| 03.08.01   | Media Storage          | Physically control and securely store system media that contain CUI.   | Functional     | Intersects With   | Data Stewardship   | DCH-01.1 | Mechanisms exist to ensure data stewardship is assigned, documented and communicated.   | 5                        |                           |
| 03.08.01   | Media Storage          | Physically control and securely store system media that contain CUI.   | Functional     | Intersects With   | Sensitive / Regulated Data Protection                                    | DCH-01.2 | Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.  | 5                        |                           |
| 03.08.01   | Media Storage          | Physically control and securely store system media that contain CUI.   | Functional     | Intersects With   | Defining Access Authorizations for Sensitive / Regulated Data            | DCH-01.4 | Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and/or physical access to sensitive/regulated data.  | 5                        |                           |
| 03.08.01   | Media Storage          | Physically control and securely store system media that contain CUI.   | Functional     | Intersects With   | Data & Asset Classification  | DCH-02   | Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.  | 5                        |                           |
| 03.08.01   | Media Storage          | Physically control and securely store system media that contain CUI.   | Functional     | Intersects With   | Media Access   | DCH-03   | Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.   | 5                        |                           |
| 03.08.01   | Media Storage          | Physically control and securely store system media that contain CUI.   | Functional     | Intersects With   | Media Storage  | DCH-06   | Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures. | 5                        |                           |
| 03.08.01   | Media Storage          | Physically control and securely store system media that contain CUI.   | Functional     | Intersects With   | Physically Secure All Media  | DCH-06.1 | Mechanisms exist to physically secure all media that contains sensitive information.  | 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   |
|---------------|--|---|----------------|-------------------|---|----------|--|--------------------------|---|
| 03.08.01      | Media Storage                            | Physically control and securely store system media that contain CUI.  | Functional     | Intersects With   | Making Sensitive Data Unreadable in Storage                   | DCH-06.4 | Mechanisms exist to ensure sensitive/regulatory data is rendered human unreadable anywhere sensitive/regulatory data is stored.  | 5                        |   |
| 03.08.01      | Media Storage                            | Physically control and securely store system media that contain CUI.  | Functional     | Intersects With   | Physical & Environmental Protections                          | PE5-01   | Mechanisms exist to facilitate the operation of physical and environmental protection controls.  | 3                        |   |
| 03.08.01      | Media Storage                            | Physically control and securely store system media that contain CUI.  | Functional     | Intersects With   | Physical Access Authorizations                                | PE5-02   | 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).                                | 3                        |   |
| 03.08.01      | Media Storage                            | Physically control and securely store system media that contain CUI.  | Functional     | Intersects With   | Role-Based Physical Access                                    | PE5-02.1 | Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.   | 3                        |   |
| 03.08.01      | Media Storage                            | Physically control and securely store system media that contain CUI.  | Functional     | Intersects With   | Physical Security of Offices, Rooms & Facilities              | PE5-04   | Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.                        | 8                        |   |
| 03.08.01      | Media Storage                            | Physically control and securely store system media that contain CUI.  | Functional     | Intersects With   | Working in Secure Areas                                       | PE5-04.1 | Physical security mechanisms exist to allow only authorized personnel access to secure areas.  | 8                        |   |
| 03.08.02      | Media Access                             | Restrict access to CUI on system media to authorized personnel or roles.  | Functional     | Intersects With   | Sensitive / Regulated Data Protection                         | DCH-01.2 | Mechanisms exist to protect sensitive/regulatory data wherever it is processed and/or stored.  | 5                        |   |
| 03.08.02      | Media Access                             | Restrict access to CUI on system media to authorized personnel or roles.  | Functional     | Intersects With   | Defining Access Authorizations for Sensitive / Regulated Data | DCH-01.4 | Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and/or physical access to sensitive/regulatory data.  | 5                        |   |
| 03.08.02      | Media Access                             | Restrict access to CUI on system media to authorized personnel or roles.  | Functional     | Subset Of         | Media Access  | DCH-03   | Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.  | 10                       |   |
| 03.08.02      | Media Access                             | Restrict access to CUI on system media to authorized personnel or roles.  | Functional     | Intersects With   | Defined Roles & Responsibilities                              | HR5-03   | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.   | 3                        |   |
| 03.08.02      | Media Access                             | Restrict access to CUI on system media to authorized personnel or roles.  | Functional     | Intersects With   | Physical & Environmental Protections                          | PE5-01   | Mechanisms exist to facilitate the operation of physical and environmental protection controls.  | 3                        |   |
| 03.08.02      | Media Access                             | Restrict access to CUI on system media to authorized personnel or roles.  | Functional     | Intersects With   | Physical Access Authorizations                                | PE5-02   | 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).                                | 3                        |   |
| 03.08.02      | Media Access                             | Restrict access to CUI on system media to authorized personnel or roles.  | Functional     | Intersects With   | Role-Based Physical Access                                    | PE5-02.1 | Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.   | 3                        |   |
| 03.08.02      | Media Access                             | Restrict access to CUI on system media to authorized personnel or roles.  | Functional     | Intersects With   | Physical Security of Offices, Rooms & Facilities              | PE5-04   | Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.                        | 3                        |   |
| 03.08.02      | Media Access                             | Restrict access to CUI on system media to authorized personnel or roles.  | Functional     | Intersects With   | Working in Secure Areas                                       | PE5-04.1 | Physical security mechanisms exist to allow only authorized personnel access to secure areas.  | 3                        |   |
| 03.08.03      | Media Sanitization                       | Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse.  | Functional     | Intersects With   | Secure Disposal, Destruction or Re-Use of Equipment           | AST-09   | Mechanisms exist to securely dispose of, destroy or repackage system components using organization-defined techniques and methods to prevent information being recovered from these components.  | 8                        |   |
| 03.08.03      | Media Sanitization                       | Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse.  | Functional     | Intersects With   | Physical Media Disposal                                       | DCH-08   | Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.  | 8                        |   |
| 03.08.03      | Media Sanitization                       | Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse.  | Functional     | Intersects With   | System Media Sanitization                                     | DCH-09   | Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.                                | 8                        |   |
| 03.08.03      | Media Sanitization                       | Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse.  | Functional     | Intersects With   | Information Disposal  | DCH-21   | Mechanisms exist to securely dispose of, destroy or erase information.   | 8                        |   |
| 03.08.04      | Media Marking                            | Mark system media that contain CUI to indicate distribution limitations, handling caveats, and applicable CUI markings. | Functional     | Intersects With   | Data & Asset Classification                                   | DCH-02   | Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.   | 8                        |   |
| 03.08.04      | Media Marking                            | Mark system media that contain CUI to indicate distribution limitations, handling caveats, and applicable CUI markings. | Functional     | Intersects With   | Media Marking   | DCH-04   | Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.   | 8                        |   |
| 03.08.05      | Media Transport                          | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control   |
| 03.08.05.a    | Media Transport                          | Protect and control system media that contain CUI during transport outside of controlled areas.                         | Functional     | Intersects With   | Data Stewardship  | DCH-01.1 | Mechanisms exist to ensure data stewardship is assigned, documented and communicated.  | 5                        |   |
| 03.08.05.a    | Media Transport                          | Protect and control system media that contain CUI during transport outside of controlled areas.                         | Functional     | Intersects With   | Sensitive / Regulated Data Protection                         | DCH-01.2 | Mechanisms exist to protect sensitive/regulatory data wherever it is processed and/or stored.  | 5                        |   |
| 03.08.05.a    | Media Transport                          | Protect and control system media that contain CUI during transport outside of controlled areas.                         | Functional     | Intersects With   | 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.  | 8                        |   |
| 03.08.05.a    | Media Transport                          | Protect and control system media that contain CUI during transport outside of controlled areas.                         | Functional     | Intersects With   | Custodians  | DCH-07.1 | Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.  | 8                        |   |
| 03.08.05.a    | Media Transport                          | Protect and control system media that contain CUI during transport outside of controlled areas.                         | Functional     | Intersects With   | Encrypting Data In Storage Media                              | DCH-07.2 | Cryptographic mechanisms exist to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.   | 5                        |   |
| 03.08.05.b    | Media Transport                          | Maintain accountability of system media that contain CUI during transport outside of controlled areas.                  | Functional     | Intersects With   | 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.  | 5                        |   |
| 03.08.05.b    | Media Transport                          | Maintain accountability of system media that contain CUI during transport outside of controlled areas.                  | Functional     | Intersects With   | Custodians  | DCH-07.1 | Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.  | 5                        |   |
| 03.08.05.c    | Media Transport                          | Document activities associated with the transport of system media that contain CUI.                                     | Functional     | Intersects With   | Sensitive / Regulated Media Records                           | DCH-01.3 | Mechanisms exist to ensure media records for sensitive/regulatory data contain sufficient information to determine the potential impact in the event of a data loss incident.  | 8                        |   |
| 03.08.06      | Withdrawn                                | Incorporated into 03.13.08.   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control   |
| 03.08.07      | Media Use                                | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control   |
| 03.08.07.a    | Media Use                                | Restrict or prohibit the use of [Assignment: organization-defined types of system media].                               | 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                       | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.08.07.a    | Media Use                                | Restrict or prohibit the use of [Assignment: organization-defined types of system media].                               | Functional     | Subset Of         | Media Use   | DCH-10   | Mechanisms exist to restrict the use of types of digital media on systems or devices.  | 10                       | ODP Value: any removable media not managed by or on behalf of the organization  |
| 03.08.07.a    | Media Use                                | Restrict or prohibit the use of [Assignment: organization-defined types of system media].                               | Functional     | Intersects With   | Removable Media Security                                      | DCH-12   | Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.   | 3                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.08.07.b    | Media Use                                | Prohibit the use of removable system media without an identifiable owner.   | Functional     | Equal             | 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.   | 10                       |   |
| 03.08.08      | Withdrawn                                | Incorporated into 03.08.07.   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control   |
| 03.08.09      | System Backup - Cryptographic Protection | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control   |
| 03.08.09.a    | System Backup - Cryptographic Protection | Protect the confidentiality of backup information.  | Functional     | Intersects With   | Data Backups  | BCD-11   | Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). | 3                        |   |
| 03.08.09.a    | System Backup - Cryptographic Protection | Protect the confidentiality of backup information.  | Functional     | Intersects With   | Cryptographic Protection                                      | BCD-11.4 | Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.   | 8                        |   |
| 03.08.09.b    | System Backup - Cryptographic Protection | Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI at backup storage locations.           | Functional     | Equal             | Cryptographic Protection                                      | BCD-11.4 | Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.   | 10                       |   |
| 03.09.01      | Personnel Screening                      | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control   |
| 03.09.01.a    | Personnel Screening                      | Screen individuals prior to authorizing access to the system.   | Functional     | Intersects With   | Position Categorization                                       | HR5-02   | Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.   | 8                        |   |
| 03.09.01.a    | Personnel Screening                      | Screen individuals prior to authorizing access to the system.   | Functional     | Subset Of         | Personnel Screening   | HR5-04   | Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.   | 10                       |   |
| 03.09.01.a    | Personnel Screening                      | Screen individuals prior to authorizing access to the system.   | Functional     | Intersects With   | Roles With Special Protection Measures                        | HR5-04.1 | Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.   | 8                        |   |
| 03.09.01.b    | Personnel Screening                      | Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening].            | Functional     | Intersects With   | Position Categorization                                       | HR5-02   | Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.   | 8                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.09.01.b    | Personnel Screening                      | Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening].            | Functional     | Subset Of         | Personnel Screening   | HR5-04   | Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.   | 10                       | ODP Value: an organizational policy requiring rescreening when there is a significant incident, or change in status, related to an individual |
| 03.09.01.b    | Personnel Screening                      | Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening].            | Functional     | Intersects With   | Roles With Special Protection Measures                        | HR5-04.1 | Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.   | 8                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.09.02      | Personnel Termination and Transfer       | N/A   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control   |
| 03.09.02.a    | Personnel Termination and Transfer       | When individual employment is terminated:   | Functional     | Subset Of         | Personnel Transfer  | HR5-08   | 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                       |   |
| 03.09.02.a    | Personnel Termination and Transfer       | When individual employment is terminated:   | Functional     | Subset Of         | Personnel Termination   | HR5-09   | Mechanisms exist to govern the termination of individual employment.   | 10                       |   |
| 03.09.02.a.01 | Personnel Termination and Transfer       | Disable system access within [Assignment: organization-defined time period].  | Functional     | Intersects With   | High-Risk Terminations  | HR5-09.2 | Mechanisms exist to expedite the process of removing "high risk" individual's access to Technology Assets, Applications, Services and/or Data (TAASD) upon termination, as determined by management.   | 8                        | ODP Value: four (4) hours   |
| 03.09.02.a.01 | Personnel Termination and Transfer       | Disable system access within [Assignment: organization-defined time period].  | Functional     | Intersects With   | Automated Employment Status Notifications                     | HR5-09.4 | Automated mechanisms exist to notify Identity and Access Management (IAM) personnel or roles upon termination of an individual employment or contract.   | 3                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.09.02.a.01 | Personnel Termination and Transfer       | Disable system access within [Assignment: organization-defined time period].  | Functional     | Intersects With   | User Provisioning & De-Provisioning                           | IAC-07   | Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.09.02.a.01 | Personnel Termination and Transfer       | Disable system access within [Assignment: organization-defined time period].  | Functional     | Equal             | Termination of Employment                                     | IAC-07.2 | Mechanisms exist to terminate employment in a timely manner, upon termination of employment or contract.   | 10                       | ODP Value: four (4) hours   |
| 03.09.02.a.02 | Personnel Termination and Transfer       | Terminate or revoke authenticators and credentials associated with the individual, and                                  | Functional     | Intersects With   | High-Risk Terminations  | HR5-09.2 | Mechanisms exist to expedite the process of removing "high risk" individual's access to Technology Assets, Applications, Services and/or Data (TAASD) upon termination, as determined by management.   | 5                        |   |
| 03.09.02.a.02 | Personnel Termination and Transfer       | Terminate or revoke authenticators and credentials associated with the individual, and                                  | Functional     | Intersects With   | Automated Employment Status Notifications                     | HR5-09.4 | Automated mechanisms exist to notify Identity and Access Management (IAM) personnel or roles upon termination of an individual employment or contract.   | 3                        |   |
| 03.09.02.a.02 | Personnel Termination and Transfer       | Terminate or revoke authenticators and credentials associated with the individual, and                                  | Functional     | Intersects With   | User Provisioning & De-Provisioning                           | IAC-07   | Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.   | 5                        |   |
| 03.09.02.a.02 | Personnel Termination and Transfer       | Terminate or revoke authenticators and credentials associated with the individual, and                                  | 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                        |   |
| 03.09.02.a.03 | Personnel Termination and Transfer       | Retrieve security-related system property.  | Functional     | Intersects With   | Asset Ownership Assignment                                    | AST-03   | Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.                               | 5                        |   |
| 03.09.02.a.03 | Personnel Termination and Transfer       | Retrieve security-related system property.  | Functional     | Intersects With   | Accountability Information                                    | AST-03.1 | Mechanisms exist to include capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory process.  | 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  |
|---------------|------------------------------------|--|----------------|-------------------|---|----------|--|--------------------------|--|
| 03.09.02.a.03 | Personnel Termination and Transfer | Retrieve security-related system property.   | Functional     | Subset Of         | Return of Assets  | AST-10   | Mechanisms exist to ensure that employees and third-party users return all organizational assets in their possession upon termination of employment, contract or agreement.  | 10                       |  |
| 03.09.02.a.03 | Personnel Termination and Transfer | Retrieve security-related system property.   | Functional     | Intersects With   | Personnel Termination   | HRS-09   | Mechanisms exist to govern the termination of individual employment.   | 5                        |  |
| 03.09.02.a.03 | Personnel Termination and Transfer | Retrieve security-related system property.   | Functional     | Intersects With   | Asset Collection  | HRS-09.1 | Mechanisms exist to retrieve organization-owned assets upon termination of an individual's employment.   | 5                        |  |
| 03.09.02.b    | Personnel Termination and Transfer | When individuals are reassigned or transferred to other positions in the organization:   | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control  |
| 03.09.02.b.01 | Personnel Termination and Transfer | Review and confirm the ongoing operational need for current logical and physical access authorizations to the system and facility, and                                       | Functional     | Intersects With   | 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.  | 5                        |  |
| 03.09.02.b.01 | Personnel Termination and Transfer | Review and confirm the ongoing operational need for current logical and physical access authorizations to the system and facility, and                                       | Functional     | Intersects With   | Personnel Termination   | HRS-09   | Mechanisms exist to govern the termination of individual employment.   | 5                        |  |
| 03.09.02.b.01 | Personnel Termination and Transfer | Review and confirm the ongoing operational need for current logical and physical access authorizations to the system and facility, and                                       | Functional     | Intersects With   | High-Risk Terminations  | HRS-09.2 | Mechanisms exist to expedite the process of removing "high risk" individual's access to Technology Assets, Applications, Services and/or Data (TAASD) upon termination, as determined by management.   | 3                        |  |
| 03.09.02.b.02 | Personnel Termination and Transfer | Modify access authorization to correspond with any changes in operational need.  | Functional     | Intersects With   | Change of Roles & Duties                                      | IAC-07.1 | Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.  | 5                        | Was 3.9.2.b.3  |
| 03.09.02.b.02 | Personnel Termination and Transfer | Modify access authorization to correspond with any changes in operational need.  | 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                        |  |
| 03.10.01      | Physical Access Authorizations     | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control  |
| 03.10.01.a    | Physical Access Authorizations     | Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides.  | Functional     | Intersects With   | Defining Access Authorizations for Sensitive / Regulated Data | DCH-01.4 | Mechanisms exist to explicitly define authorizations for specific individuals and roles for logical and/or physical access to sensitive/regulated data.  | 8                        |  |
| 03.10.01.a    | Physical Access Authorizations     | Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides.  | Functional     | Intersects With   | Access To Sensitive / Regulated Data                          | IAC-20.1 | Mechanisms exist to limit access to sensitive/regulated data to only those individuals whose job requires such access.   | 8                        |  |
| 03.10.01.a    | Physical Access Authorizations     | Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides.  | Functional     | Intersects With   | Physical & Environmental Protections                          | PES-01   | Mechanisms exist to facilitate the operation of physical and environmental protection controls.  | 3                        |  |
| 03.10.01.a    | Physical Access Authorizations     | Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides.  | Functional     | Intersects With   | 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).                                    | 5                        |  |
| 03.10.01.b    | Physical Access Authorizations     | Issue authorization credentials for facility access.   | Functional     | Intersects With   | 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).                                    | 5                        |  |
| 03.10.01.b    | Physical Access Authorizations     | Issue authorization credentials for facility access.   | Functional     | Intersects With   | 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.   | 5                        |  |
| 03.10.01.c    | Physical Access Authorizations     | Review the facility access list [Assignment: organization-defined frequency].  | Functional     | Intersects With   | Periodic Review of Account Privileges                         | IAC-17   | Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.  | 3                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.10.01.c    | Physical Access Authorizations     | Review the facility access list [Assignment: organization-defined frequency].  | Functional     | Intersects With   | 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).                                    | 8                        | ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks   |
| 03.10.01.d    | Physical Access Authorizations     | Remove individuals from the facility access list when access is no longer required.  | Functional     | Intersects With   | Periodic Review of Account Privileges                         | IAC-17   | Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.  | 3                        |  |
| 03.10.01.d    | Physical Access Authorizations     | Remove individuals from the facility access list when access is no longer required.  | Functional     | Intersects With   | 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).                                    | 8                        |  |
| 03.10.01.d    | Physical Access Authorizations     | Remove individuals from the facility access list when access is no longer required.  | Functional     | Intersects With   | 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.   | 3                        |  |
| 03.10.02      | Monitoring Physical Access         | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control  |
| 03.10.02.a    | Monitoring Physical Access         | Monitor physical access to the facility where the system resides to detect and respond to physical security incidents.   | Functional     | Intersects With   | Physical Access Control                                       | PES-03   | Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible). | 8                        |  |
| 03.10.02.a    | Monitoring Physical Access         | Monitor physical access to the facility where the system resides to detect and respond to physical security incidents.   | Functional     | Intersects With   | Controlled Ingress & Egress Points                            | PES-03.1 | Physical access control mechanisms exist to limit and monitor physical access through controlled ingress and egress points.  | 5                        |  |
| 03.10.02.a    | Monitoring Physical Access         | Monitor physical access to the facility where the system resides to detect and respond to physical security incidents.   | Functional     | Intersects With   | Physical Access Logs  | PES-03.3 | Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.  | 8                        |  |
| 03.10.02.a    | Monitoring Physical Access         | Monitor physical access to the facility where the system resides to detect and respond to physical security incidents.   | Functional     | Subset Of         | Monitoring Physical Access                                    | PES-05   | Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.  | 10                       |  |
| 03.10.02.a    | Monitoring Physical Access         | Monitor physical access to the facility where the system resides to detect and respond to physical security incidents.   | Functional     | Intersects With   | Intrusion Alarms / Surveillance Equipment                     | PES-05.1 | Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.  | 5                        |  |
| 03.10.02.a    | Monitoring Physical Access         | Monitor physical access to the facility where the system resides to detect and respond to physical security incidents.   | Functional     | Intersects With   | Monitoring Physical Access To Critical Systems                | PES-05.2 | Facility security mechanisms exist to monitor physical access to critical systems or sensitive/regulated data, in addition to the physical access monitoring of the facility.  | 3                        |  |
| 03.10.02.b    | Monitoring Physical Access         | Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indicators of events]. | Functional     | Subset Of         | Monitoring Physical Access                                    | PES-05   | Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.  | 10                       | ODP Values: 1) at least every 45 days, 2) significant, novel incidents, or significant changes to risks.   |
| 03.10.02.b    | Monitoring Physical Access         | Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indicators of events]. | Functional     | Intersects With   | Intrusion Alarms / Surveillance Equipment                     | PES-05.1 | Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.  | 5                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.10.02.b    | Monitoring Physical Access         | Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indicators of events]. | Functional     | Intersects With   | Monitoring Physical Access To Critical Systems                | PES-05.2 | Facility security mechanisms exist to monitor physical access to critical systems or sensitive/regulated data, in addition to the physical access monitoring of the facility.  | 5                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.10.02.b    | Monitoring Physical Access         | Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indicators of events]. | Functional     | Intersects With   | Visitor Control   | PES-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).  | 5                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.10.02.b    | Monitoring Physical Access         | Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indicators of events]. | Functional     | Intersects With   | Distinguish Visitors from On-Site Personnel                   | PES-06.1 | Physical access control mechanisms exist to easily distinguish between onsite personnel and visitors, especially in areas where sensitive/regulated data is accessible.  | 5                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.10.03      | Withdrawn                          | Incorporated into 03.10.07.  | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control  |
| 03.10.04      | Withdrawn                          | Incorporated into 03.10.07.  | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control  |
| 03.10.05      | Withdrawn                          | Incorporated into 03.10.07.  | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control  |
| 03.10.06      | Alternate Work Site                | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control  |
| 03.10.06.a    | Alternate Work Site                | Determine alternate work sites allowed for use by employees.   | Functional     | Intersects With   | Work From Anywhere (WFA) - Telecommuting Security             | NET-14.5 | Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.  | 8                        |  |
| 03.10.06.a    | Alternate Work Site                | Determine alternate work sites allowed for use by employees.   | Functional     | Equal             | Alternate Work Site   | PES-11   | Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.  | 10                       |  |
| 03.10.06.b    | Alternate Work Site                | Employ the following security requirements at alternate work sites: [Assignment: organization-defined security requirements].  | Functional     | Intersects With   | Work From Anywhere (WFA) - Telecommuting Security             | NET-14.5 | Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.  | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.10.06.b    | Alternate Work Site                | Employ the following security requirements at alternate work sites: [Assignment: organization-defined security requirements].  | Functional     | Intersects With   | Alternate Work Site   | PES-11   | Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.  | 8                        | ODP Value: adequate security, comparable to organizational security requirements at the primary work site where practical, documented in policy, and covered by training |
| 03.10.07      | Physical Access Control            | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control  |
| 03.10.07.a    | Physical Access Control            | Enforce physical access authorizations at entry and exit points to the facility where the system resides by:   | Functional     | Subset Of         | Physical & Environmental Protections                          | PES-01   | Mechanisms exist to facilitate the operation of physical and environmental protection controls.  | 10                       |  |
| 03.10.07.a    | Physical Access Control            | Enforce physical access authorizations at entry and exit points to the facility where the system resides by:   | Functional     | Intersects With   | 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).                                    | 5                        |  |
| 03.10.07.a    | Physical Access Control            | Enforce physical access authorizations at entry and exit points to the facility where the system resides by:   | Functional     | Intersects With   | Physical Access Control                                       | PES-03   | Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible). | 5                        |  |
| 03.10.07.a    | Physical Access Control            | Enforce physical access authorizations at entry and exit points to the facility where the system resides by:   | Functional     | Intersects With   | Controlled Ingress & Egress Points                            | PES-03.1 | Physical access control mechanisms exist to limit and monitor physical access through controlled ingress and egress points.  | 8                        |  |
| 03.10.07.a.01 | Physical Access Control            | Verifying individual physical access authorizations before granting access to the facility and   | Functional     | Intersects With   | Physical Access Control                                       | PES-03   | Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible). | 5                        |  |
| 03.10.07.a.01 | Physical Access Control            | Verifying individual physical access authorizations before granting access to the facility and   | Functional     | Intersects With   | Access To Critical Systems                                    | PES-03.4 | Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulated data, in addition to the physical access controls for the facility.   | 3                        |  |
| 03.10.07.a.01 | Physical Access Control            | Verifying individual physical access authorizations before granting access to the facility and   | Functional     | Intersects With   | Physical Security of Offices, Rooms & Facilities              | PES-04   | Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.                            | 3                        |  |
| 03.10.07.a.01 | Physical Access Control            | Verifying individual physical access authorizations before granting access to the facility and   | Functional     | Intersects With   | Working in Secure Areas                                       | PES-04.1 | Physical security mechanisms exist to allow only authorized personnel access to secure areas.  | 3                        |  |
| 03.10.07.a.02 | Physical Access Control            | Controlling ingress and egress with physical access control systems, devices, or 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                       |  |
| 03.10.07.a.02 | Physical Access Control            | Controlling ingress and egress with physical access control systems, devices, or guards.   | Functional     | Intersects With   | Controlled Ingress & Egress Points                            | PES-03.1 | Physical access control mechanisms exist to limit and monitor physical access through controlled ingress and egress points.  | 8                        |  |
| 03.10.07.a.02 | Physical Access Control            | Controlling ingress and egress with physical access control systems, devices, or guards.   | Functional     | Intersects With   | Access To Critical Systems                                    | PES-03.4 | Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulated data, in addition to the physical access controls for the facility.   | 3                        |  |
| 03.10.07.a.02 | Physical Access Control            | Controlling ingress and egress with physical access control systems, devices, or guards.   | Functional     | Intersects With   | Physical Security of Offices, Rooms & Facilities              | PES-04   | Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.                            | 3                        |  |

| 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   |
|---------------|---------------------------------------|--|----------------|-------------------|--|----------|---|--------------------------|---|
| 03.10.07.a.02 | Physical Access Control               | Controlling ingress and egress with physical access control systems, devices, or guards.   | Functional     | Intersects With   | Working in Secure Areas                          | PE-04.1  | Physical security mechanisms exist to allow only authorized personnel access to secure areas.   | 3                        |   |
| 03.10.07.b    | Physical Access Control               | Maintain physical access audit logs for entry or exit points.  | Functional     | Equal             | 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                       |   |
| 03.10.07.c    | Physical Access Control               | Escort visitors, and control 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                       |   |
| 03.10.07.c    | Physical Access Control               | Escort visitors, and control visitor activity.   | Functional     | Intersects With   | Distinguish Visitors from On-Site Personnel      | PE-06.1  | Physical access control mechanisms exist to easily distinguish between onsite personnel and visitors, especially in areas where sensitive/unclassified data is accessible.  | 5                        |   |
| 03.10.07.c    | Physical Access Control               | Escort visitors, and control visitor activity.   | Functional     | Intersects With   | Identification Requirement                       | PE-06.2  | Physical access control mechanisms exist to require at least one(1) form of government-issued or organization-issued photo identification to authenticate individuals before they can gain access to the facility.  | 5                        |   |
| 03.10.07.c    | Physical Access Control               | Escort visitors, and control visitor activity.   | Functional     | Intersects With   | Restrict Unescorted Access                       | PE-06.3  | Physical access control mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access.   | 8                        |   |
| 03.10.07.c    | Physical Access Control               | Escort visitors, and control visitor activity.   | Functional     | Intersects With   | Visitor Access Revocation                        | PE-06.6  | Mechanisms exist to ensure visitor badges, or other issued identification, are surrendered before visitors leave the facility or are deactivated at a pre-determined time/date of expiration.   | 5                        |   |
| 03.10.07.d    | Physical Access Control               | Secure keys, combinations, and other physical access devices.  | 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                       |   |
| 03.10.07.d    | Physical Access Control               | Secure keys, combinations, and other physical access devices.  | Functional     | Intersects With   | Physical Security of Offices, Rooms & Facilities | PE-04    | Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.   | 3                        |   |
| 03.10.07.d    | Physical Access Control               | Secure keys, combinations, and other physical access devices.  | Functional     | Intersects With   | Working in Secure Areas                          | PE-04.1  | Physical security mechanisms exist to allow only authorized personnel access to secure areas.   | 3                        |   |
| 03.10.07.e    | Physical Access Control               | Control physical access to output devices to prevent unauthorized individuals from obtaining access to CUI.  | 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                        |   |
| 03.10.07.e    | Physical Access Control               | Control physical access to output devices to prevent unauthorized individuals from obtaining access to CUI.  | Functional     | Intersects With   | 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.  | 5                        |   |
| 03.10.08      | Access Control for Transmission       | Control physical access to system distribution and transmission lines within organizational facilities.  | Functional     | Intersects With   | Supporting Utilities                             | PE-07    | Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.   | 5                        |   |
| 03.10.08      | Access Control for Transmission       | Control physical access to system distribution and transmission lines within organizational facilities.  | 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                        |   |
| 03.10.08      | Access Control for Transmission       | Control physical access to system distribution and transmission lines within organizational facilities.  | Functional     | Intersects With   | 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.  | 5                        |   |
| 03.11.01      | Risk Assessment                       | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control   |
| 03.11.01.a    | Risk Assessment                       | Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI.                       | Functional     | Intersects With   | Prohibited Equipment & Services                  | AST-17   | Mechanisms exist to govern Supply Chain Risk Management (SCRM) sanctions that require the removal and prohibition of certain Technology Assets, Applications and/or Services (TAAS) that are designated as supply chain threats by a statutory or regulatory body.  | 3                        |   |
| 03.11.01.a    | Risk Assessment                       | Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI.                       | Functional     | Subset Of         | Risk Management Program                          | RSK-01   | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.  | 10                       |   |
| 03.11.01.a    | Risk Assessment                       | Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI.                       | Functional     | Intersects With   | Risk Framing                                     | RSK-01.1 | Mechanisms exist to identify:<br>1) Assumptions affecting risk assessments, risk response and risk monitoring;<br>2) Constraints affecting risk assessments, risk response and risk monitoring;<br>3) The organizational risk tolerance; and<br>4) Priorities, benefits and trade-offs considered by the organization for managing risk.  | 8                        |   |
| 03.11.01.a    | Risk Assessment                       | Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI.                       | Functional     | Intersects With   | 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:<br>1) Document the security categorization results (including supporting rationale) in the security plan for systems; and<br>2) Ensure the security categorization decision is reviewed and approved by the asset owner. | 5                        |   |
| 03.11.01.a    | Risk Assessment                       | Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI.                       | Functional     | Intersects With   | Impact-Level Prioritization                      | RSK-02.1 | Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.  | 3                        |   |
| 03.11.01.a    | Risk Assessment                       | Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI.                       | Functional     | Intersects With   | Risk Identification                              | RSK-03   | Mechanisms exist to identify and document risks, both internal and external.  | 5                        |   |
| 03.11.01.a    | Risk Assessment                       | Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI.                       | Functional     | Intersects With   | Risk Assessment                                  | RSK-04   | Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).   | 8                        |   |
| 03.11.01.a    | Risk Assessment                       | Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI.                       | Functional     | Intersects With   | Risk Ranking                                     | RSK-05   | Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices.   | 5                        |   |
| 03.11.01.a    | Risk Assessment                       | Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI.                       | Functional     | Intersects With   | Supply Chain Risk Management (SCRM) Plan         | RSK-09   | Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.  | 5                        |   |
| 03.11.01.a    | Risk Assessment                       | Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI.                       | Functional     | Intersects With   | Supply Chain Risk Assessment                     | RSK-09.1 | Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).  | 8                        |   |
| 03.11.01.a    | Risk Assessment                       | Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI.                       | Functional     | Intersects With   | Third-Party Criticality Assessments              | TPM-02   | Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.  | 3                        |   |
| 03.11.01.a    | Risk Assessment                       | Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI.                       | Functional     | Intersects With   | Supply Chain Risk Management (SCRM)              | TPM-03   | Mechanisms exist to:<br>1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and<br>2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.   | 3                        |   |
| 03.11.01.a    | Risk Assessment                       | Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI.                       | Functional     | Intersects With   | 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).   | 8                        |   |
| 03.11.01.b    | Risk Assessment                       | Update risk assessments (Assignment: organization-defined frequency).  | Functional     | Equal             | Risk Assessment Update                           | RSK-07   | Mechanisms exist to routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.  | 10                       | ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks  |
| 03.11.01.b    | Risk Assessment                       | Update risk assessments (Assignment: organization-defined frequency).  | Functional     | Intersects With   | Supply Chain Risk Assessment                     | RSK-09.1 | Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).  | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.11.02      | Vulnerability Monitoring and Scanning | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control   |
| 03.11.02.a    | Vulnerability Monitoring and Scanning | Monitor and scan the system for vulnerabilities (Assignment: organization-defined frequency) and when new vulnerabilities affecting the system are identified. | 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.   | 3                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.11.02.a    | Vulnerability Monitoring and Scanning | Monitor and scan the system for vulnerabilities (Assignment: organization-defined frequency) and when new vulnerabilities affecting the system are identified. | Functional     | Intersects With   | Threat Intelligence Feeds                        | THR-03   | Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.   | 8                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.11.02.a    | Vulnerability Monitoring and Scanning | Monitor and scan the system for vulnerabilities (Assignment: organization-defined frequency) and when new vulnerabilities affecting the system are identified. | Functional     | Subset Of         | Vulnerability & Patch Management Program (VPMF)  | VPM-01   | Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.  | 10                       | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.11.02.a    | Vulnerability Monitoring and Scanning | Monitor and scan the system for vulnerabilities (Assignment: organization-defined frequency) and when new vulnerabilities affecting the system are identified. | Functional     | Intersects With   | Attack Surface Scope                             | VPM-01.1 | Mechanisms exist to define and manage the scope for its attack surface management activities.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.11.02.a    | Vulnerability Monitoring and Scanning | Monitor and scan the system for vulnerabilities (Assignment: organization-defined frequency) and when new vulnerabilities affecting the system are identified. | Functional     | Intersects With   | Vulnerability Ranking                            | VPM-03   | Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.   | 8                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.11.02.a    | Vulnerability Monitoring and Scanning | Monitor and scan the system for vulnerabilities (Assignment: organization-defined frequency) and when new vulnerabilities affecting the system are identified. | Functional     | Intersects With   | Vulnerability Scanning and Reporting             | VPM-06   | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.  | 8                        | ODP Value: at least monthly, or when there are significant incidents or significant changes to risks  |
| 03.11.02.b    | Vulnerability Monitoring and Scanning | Remediate system vulnerabilities within (Assignment: organization-defined response times).   | Functional     | Intersects With   | Risk Remediation                                 | RSK-06   | Mechanisms exist to remediate risks to an acceptable level.   | 8                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.11.02.b    | Vulnerability Monitoring and Scanning | Remediate system vulnerabilities within (Assignment: organization-defined response times).   | Functional     | Intersects With   | Risk Response                                    | RSK-06.1 | performed to remediate findings from security, compliance and/or resilience-related:<br>1) Assessments;<br>2) Audits; and<br>3) Assessments.  | 8                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.11.02.b    | Vulnerability Monitoring and Scanning | Remediate system vulnerabilities within (Assignment: organization-defined response times).   | Functional     | Intersects With   | Compensating Countermeasures                     | RSK-06.2 | Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.   | 3                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.11.02.b    | Vulnerability Monitoring and Scanning | Remediate system vulnerabilities within (Assignment: organization-defined response times).   | Functional     | Subset Of         | Vulnerability Remediation Process                | VPM-02   | Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.  | 10                       | ODP Value: thirty (30) days from date of discovery for high-risk vulnerabilities (including both critical and high); 90 days from date of discovery for moderate-risk vulnerabilities; and 180 days from date of discovery for low-risk vulnerabilities |
| 03.11.02.b    | Vulnerability Monitoring and Scanning | Remediate system vulnerabilities within (Assignment: organization-defined response times).   | Functional     | Intersects With   | Continuous Vulnerability Remediation Activities  | VPM-04   | Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.  | 8                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.11.02.b    | Vulnerability Monitoring and Scanning | Remediate system vulnerabilities within (Assignment: organization-defined response times).   | 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.  | 8                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.11.02.c    | Vulnerability Monitoring and Scanning | Update system vulnerabilities to be scanned (Assignment: organization-defined frequency) and when new vulnerabilities are identified and reported.             | Functional     | Equal             | Update Tool Capability                           | VPM-06.1 | Mechanisms exist to update vulnerability scanning tools.  | 10                       | ODP Value: no more than 24 hours prior to running the scans   |
| 03.11.03      | Withdrawn                             | Incorporated into 03.11.02.  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control   |
| 03.11.04      | Risk Response                         | Respond to findings from security assessments, monitoring, and audits.   | Functional     | Subset Of         | Risk Response                                    | RSK-06.1 | performed to remediate findings from security, compliance and/or resilience-related:<br>1) Assessments;<br>2) Audits; and<br>3) Assessments.  | 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  |
|---------------|-------------------------------|--|----------------|-------------------|--|----------|--|--------------------------|--|
| 03.12.01      | Security Assessment           | Assess the security requirements for the system and its environment of operation (Assignment: organization-defined frequency) to determine if the requirements have been satisfied.  | 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                       | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.12.01      | Security Assessment           | Assess the security requirements for the system and its environment of operation (Assignment: organization-defined frequency) to determine if the requirements have been satisfied.  | 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.   | 8                        | ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks |
| 03.12.01      | Security Assessment           | Assess the security requirements for the system and its environment of operation (Assignment: organization-defined frequency) to determine if the requirements have been satisfied.  | Functional     | Intersects With   | Internal Audit Function  | CPL-02.1 | Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.   | 3                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.12.01      | Security Assessment           | Assess the security requirements for the system and its environment of operation (Assignment: organization-defined frequency) to determine if the requirements have been satisfied.  | 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.  | 8                        | ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks |
| 03.12.01      | Security Assessment           | Assess the security requirements for the system and its environment of operation (Assignment: organization-defined frequency) to determine if the requirements have been satisfied.  | 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                       | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.12.01      | Security Assessment           | Assess the security requirements for the system and its environment of operation (Assignment: organization-defined frequency) to determine if the requirements have been satisfied.  | Functional     | Intersects With   | Assessment Boundaries  | IAO-01.1 | Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.  | 5                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.12.01      | Security Assessment           | Assess the security requirements for the system and its environment of operation (Assignment: organization-defined frequency) to determine if the requirements have been satisfied.  | 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.  | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.12.01      | Security Assessment           | Assess the security requirements for the system and its environment of operation (Assignment: organization-defined frequency) to determine if the requirements have been satisfied.  | Functional     | Intersects With   | Technology Development & Acquisition                             | TDA-01   | Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.  | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.12.01      | Security Assessment           | Assess the security requirements for the system and its environment of operation (Assignment: organization-defined frequency) to determine if the requirements have been satisfied.  | Functional     | Intersects With   | Security, Compliance & Resilience Testing Throughout Development | TDA-09   | Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:<br>(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;<br>(2) Implement a verifiable flow remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and<br>(3) Document the results.   | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.12.02      | Plan of Action and Milestones | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A  | 0                        | No applicable SCF control  |
| 03.12.02.a    | Plan of Action and Milestones | Develop a plan of action and milestones for the system:  | Functional     | Subset Of         | Capabilities Deficiency Tracking                                 | IAO-05   | (2) Applicable security, compliance and/or resilience control;<br>(3) Description of the deficiency(ies);<br>(4) Risk associated with the deficiency(ies);<br>(5) Source deficiency identification/detection;<br>(6) Temporary compensating controls, if applicable;<br>(7) Point of Contact (POC) (e.g., asset/process owner);<br>(8) Remediation plan, or similar capability.  | 10                       |  |
| 03.12.02.a.01 | Plan of Action and Milestones | To document the planned remediation actions to correct weaknesses or deficiencies noted during security assessments and  | Functional     | Intersects With   | Non-Compliance Oversight   | CPL-01.1 | Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.  | 3                        |  |
| 03.12.02.a.01 | Plan of Action and Milestones | To document the planned remediation actions to correct weaknesses or deficiencies noted during security assessments and  | Functional     | Subset Of         | Capabilities Deficiency Tracking                                 | IAO-05   | (2) Applicable security, compliance and/or resilience control;<br>(3) Description of the deficiency(ies);<br>(4) Risk associated with the deficiency(ies);<br>(5) Source deficiency identification/detection;<br>(6) Temporary compensating controls, if applicable;<br>(7) Point of Contact (POC) (e.g., asset/process owner);<br>(8) Remediation plan, or similar capability.  | 10                       |  |
| 03.12.02.a.01 | Plan of Action and Milestones | To document the planned remediation actions to correct weaknesses or deficiencies noted during security assessments and  | Functional     | Intersects With   | Risk Register  | RSK-04.1 | Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.   | 3                        |  |
| 03.12.02.a.02 | Plan of Action and Milestones | To reduce or eliminate known system vulnerabilities.   | Functional     | Subset Of         | Capabilities Deficiency Tracking                                 | IAO-05   | (2) Applicable security, compliance and/or resilience control;<br>(3) Description of the deficiency(ies);<br>(4) Risk associated with the deficiency(ies);<br>(5) Source deficiency identification/detection;<br>(6) Temporary compensating controls, if applicable;<br>(7) Point of Contact (POC) (e.g., asset/process owner);<br>(8) Remediation plan, or similar capability.  | 10                       |  |
| 03.12.02.a.02 | Plan of Action and Milestones | To reduce or eliminate known system vulnerabilities.   | Functional     | Intersects With   | Risk Register  | RSK-04.1 | Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.   | 3                        |  |
| 03.12.02.a.02 | Plan of Action and Milestones | To reduce or eliminate known system vulnerabilities.   | Functional     | Intersects With   | Risk Remediation   | RSK-06   | Mechanisms exist to remediate risks to an acceptable level.  | 5                        |  |
| 03.12.02.a.02 | Plan of Action and Milestones | To reduce or eliminate known system vulnerabilities.   | Functional     | Subset Of         | Vulnerability Remediation Process                                | VPM-02   | Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.   | 10                       |  |
| 03.12.02.a.02 | Plan of Action and Milestones | To reduce or eliminate known system vulnerabilities.   | 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.   | 3                        |  |
| 03.12.02.b    | Plan of Action and Milestones | Update the existing plan of action and milestones based on the findings from:  | Functional     | Subset Of         | Capabilities Deficiency Tracking                                 | IAO-05   | (2) Applicable security, compliance and/or resilience control;<br>(3) Description of the deficiency(ies);<br>(4) Risk associated with the deficiency(ies);<br>(5) Source deficiency identification/detection;<br>(6) Temporary compensating controls, if applicable;<br>(7) Point of Contact (POC) (e.g., asset/process owner);<br>(8) Remediation plan, or similar capability.  | 10                       |  |
| 03.12.02.b.01 | Plan of Action and Milestones | Security assessments,  | Functional     | Subset Of         | Capabilities Deficiency Tracking                                 | IAO-05   | (2) Applicable security, compliance and/or resilience control;<br>(3) Description of the deficiency(ies);<br>(4) Risk associated with the deficiency(ies);<br>(5) Source deficiency identification/detection;<br>(6) Temporary compensating controls, if applicable;<br>(7) Point of Contact (POC) (e.g., asset/process owner);<br>(8) Remediation plan, or similar capability.  | 10                       |  |
| 03.12.02.b.02 | Plan of Action and Milestones | Audits or reviews, and   | Functional     | Subset Of         | Capabilities Deficiency Tracking                                 | IAO-05   | (2) Applicable security, compliance and/or resilience control;<br>(3) Description of the deficiency(ies);<br>(4) Risk associated with the deficiency(ies);<br>(5) Source deficiency identification/detection;<br>(6) Temporary compensating controls, if applicable;<br>(7) Point of Contact (POC) (e.g., asset/process owner);<br>(8) Remediation plan, or similar capability.  | 10                       |  |
| 03.12.02.b.03 | Plan of Action and Milestones | Continuous monitoring activities.  | Functional     | Subset Of         | Capabilities Deficiency Tracking                                 | IAO-05   | (2) Applicable security, compliance and/or resilience control;<br>(3) Description of the deficiency(ies);<br>(4) Risk associated with the deficiency(ies);<br>(5) Source deficiency identification/detection;<br>(6) Temporary compensating controls, if applicable;<br>(7) Point of Contact (POC) (e.g., asset/process owner);<br>(8) Remediation plan, or similar capability.  | 10                       |  |
| 03.12.03      | Continuous Monitoring         | Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and security assessments.   | 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                        |  |
| 03.12.03      | Continuous Monitoring         | Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and security assessments.   | 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.  | 8                        |  |
| 03.12.03      | Continuous Monitoring         | Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and security assessments.   | 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                        |  |
| 03.12.03      | Continuous Monitoring         | Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and security assessments.   | Functional     | Intersects With   | Steering Committee & Program Oversight                           | GOV-01.1 | Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.  | 5                        |  |
| 03.12.03      | Continuous Monitoring         | Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and security assessments.   | Functional     | Intersects With   | Status Reporting To Governing Body                               | GOV-01.2 | Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).  | 5                        |  |
| 03.12.03      | Continuous Monitoring         | Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and security assessments.   | Functional     | Intersects With   | Measures of Performance  | GOV-05   | Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.  | 5                        |  |
| 03.12.03      | Continuous Monitoring         | Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and security assessments.   | Functional     | Intersects With   | Continuous Monitoring  | MON-01   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.  | 5                        |  |
| 03.12.03      | Continuous Monitoring         | Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and security assessments.   | Functional     | Intersects With   | Technology Development & Acquisition                             | TDA-01   | Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.  | 5                        |  |
| 03.12.03      | Continuous Monitoring         | Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and security assessments.   | Functional     | Intersects With   | Product Management   | TDA-01.1 | Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:<br>(1) Improve functionality;<br>(2) Enhance security and resiliency capabilities;<br>(3) Correct security deficiencies; and<br>(4) Conform with applicable statutory, regulatory and/or contractual obligations. | 3                        |  |
| 03.12.03      | Continuous Monitoring         | Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and security assessments.   | Functional     | Intersects With   | Security, Compliance & Resilience Testing Throughout Development | TDA-09   | Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:<br>(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;<br>(2) Implement a verifiable flow remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and<br>(3) Document the results.   | 5                        |  |
| 03.12.03      | Continuous Monitoring         | Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and security assessments.   | Functional     | Intersects With   | Continuous Monitoring Plan                                       | TDA-09.1 | Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a plan for the continuous monitoring of security, compliance and/or resilience control effectiveness.  | 5                        |  |
| 03.12.04      | Withdrawn                     | Incorporated into 03.15.02.  | Functional     | No Relationship   | N/A  | N/A      | N/A  | 0                        | No applicable SCF control  |
| 03.12.05      | Information Exchange          | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A  | 0                        | No applicable SCF control  |
| 03.12.05.a    | Information Exchange          | Approve and manage the exchange of CUI between the system and other systems using Selection (one or more); interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service-level agreements; user agreements; non-disclosure agreements; other types of agreements). | Functional     | Intersects With   | Transfer Authorizations  | DCH-14.2 | Mechanisms exist to verify that individuals or Technology Assets, Applications and/or Services (TAAS) transferring data between interconnecting TAAS have the requisite authorizations (e.g., write permissions or privileges) prior to transferring said data.  | 8                        | ODP Value: requirements as described in the contract   |
| 03.12.05.a    | Information Exchange          | Approve and manage the exchange of CUI between the system and other systems using Selection (one or more); interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service-level agreements; user agreements; non-disclosure agreements; other types of agreements). | Functional     | Intersects With   | Data Access Mapping  | DCH-14.3 | Mechanisms exist to leverage data-specific Access Control Lists (ACLs), Interconnection Security Agreements (ISAs) to generate a logical map of the parties with whom sensitive/regulate data is shared.   | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.12.05.a    | Information Exchange          | Approve and manage the exchange of CUI between the system and other systems using Selection (one or more); interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service-level agreements; user agreements; non-disclosure agreements; other types of agreements). | Functional     | Intersects With   | Access Agreements  | HR5-06   | Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.  | 8                        | DoD-provided ODP does not apply to this specific 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   |
|------------|--|--|----------------|-------------------|--|----------|--|--------------------------|---|
| 03.12.05.a | Information Exchange   | Approve and manage the exchange of CUI between the system and other systems using Selection (one or more); interconnection security agreements; information exchange security agreements; memoranda of understanding or agreements; service-level agreements; user agreements; non-disclosure agreements; other types of agreements. | Functional     | Intersects With   | Confidentiality Agreements                                     | HRS-06.1 | Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar contracts that reflect the needs to protect data and operational details, or both employees and third-parties.   | 3                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.12.05.a | Information Exchange   | Approve and manage the exchange of CUI between the system and other systems using Selection (one or more); interconnection security agreements; information exchange security agreements; memoranda of understanding or agreements; service-level agreements; user agreements; non-disclosure agreements; other types of agreements. | 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.              | 8                        | ODP Value: requirements as described in the contract  |
| 03.12.05.a | Information Exchange   | Approve and manage the exchange of CUI between the system and other systems using Selection (one or more); interconnection security agreements; information exchange security agreements; memoranda of understanding or agreements; service-level agreements; user agreements; non-disclosure agreements; other types of agreements. | Functional     | Intersects With   | 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.  | 8                        | ODP Value: requirements as described in the contract  |
| 03.12.05.b | Information Exchange   | Document interface characteristics, security requirements, and responsibilities for each system as part of the exchange agreements.  | 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.              | 8                        |   |
| 03.12.05.b | Information Exchange   | Document interface characteristics, security requirements, and responsibilities for each system as part of the exchange agreements.  | Functional     | Intersects With   | 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.  | 8                        |   |
| 03.12.05.c | Information Exchange   | Review and update the exchange agreements (Assignment: organization-defined frequency).  | 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                       | ODP Value: at least every 12 months   |
| 03.13.01   | Boundary Protection  | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A  | 0                        | No applicable SCF control   |
| 03.13.01.a | Boundary Protection  | Monitor and control communications at external managed interfaces to the system and key internal managed interfaces within the system.   | Functional     | Intersects With   | 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.  | 8                        |   |
| 03.13.01.a | Boundary Protection  | Monitor and control communications at external managed interfaces to the system and key internal managed interfaces within the system.   | Functional     | Intersects With   | Inbound & Outbound Communications Traffic                      | MON-01.3 | Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.   | 8                        |   |
| 03.13.01.a | Boundary Protection  | Monitor and control communications at external managed interfaces to the system and key internal managed interfaces within the system.   | 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                       |   |
| 03.13.01.a | Boundary Protection  | Monitor and control communications at external managed interfaces to the system and key internal managed interfaces within the system.   | Functional     | Intersects With   | Boundary Protection  | NET-03   | Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.   | 8                        |   |
| 03.13.01.a | Boundary Protection  | Monitor and control communications at external managed interfaces to the system and key internal managed interfaces within the system.   | Functional     | Intersects With   | 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.   | 8                        |   |
| 03.13.01.a | Boundary Protection  | Monitor and control communications at external managed interfaces to the system and key internal managed interfaces within the system.   | 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).  | 8                        |   |
| 03.13.01.a | Boundary Protection  | Monitor and control communications at external managed interfaces to the system and key internal managed interfaces within the system.   | Functional     | Intersects With   | Network Intrusion Detection / Prevention Systems (NIDS / NIPS) | NET-08   | Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.  | 8                        |   |
| 03.13.01.b | Boundary Protection  | Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.   | Functional     | Subset Of         | Layered Network Defenses                                       | NET-02   | Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.   | 10                       |   |
| 03.13.01.b | Boundary Protection  | Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.   | Functional     | Intersects With   | Boundary Protection  | NET-03   | Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.   | 5                        |   |
| 03.13.01.b | Boundary Protection  | Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.   | Functional     | Intersects With   | Separate Subnet for Connecting to Different Security Domains   | NET-03.8 | Mechanisms exist to implement separate network addresses (e.g., different subnets) to connect to systems in different security domains.  | 3                        |   |
| 03.13.01.b | Boundary Protection  | Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.   | Functional     | Subset Of         | Network Segmentation (macrosegmentation)                       | NET-06   | Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.   | 10                       |   |
| 03.13.01.b | Boundary Protection  | Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.   | Functional     | Intersects With   | Sensitive / Regulated Data Enclave (Secure Zone)               | NET-06.3 | Mechanisms exist to implement segmentation controls to restrict inbound and outbound connectivity for sensitive/regulated data enclaves (secure zones).  | 8                        |   |
| 03.13.01.b | Boundary Protection  | Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.   | Functional     | Intersects With   | DMZ Networks   | NET-08.1 | Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.   | 8                        |   |
| 03.13.01.c | Boundary Protection  | Connect to external systems only through managed interfaces that consist of boundary protection devices arranged in accordance with an organizational security architecture.   | Functional     | Intersects With   | Boundary Protection  | NET-03   | Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.   | 5                        |   |
| 03.13.01.c | Boundary Protection  | Connect to external systems only through managed interfaces that consist of boundary protection devices arranged in accordance with an organizational security architecture.   | Functional     | Intersects With   | 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.   | 5                        |   |
| 03.13.01.c | Boundary Protection  | Connect to external systems only through managed interfaces that consist of boundary protection devices arranged in accordance with an organizational security architecture.   | 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).   | 3                        |   |
| 03.13.01.c | Boundary Protection  | Connect to external systems only through managed interfaces that consist of boundary protection devices arranged in accordance with an organizational security architecture.   | 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.   | 8                        |   |
| 03.13.02   | Boundary Protection  | Recategorized as NCD.  | Functional     | No Relationship   | N/A  | N/A      | N/A  | 0                        | No applicable SCF control   |
| 03.13.03   | Withdrawn  | Addressed by 03.01.01, 03.01.02, 03.01.03, 03.01.04, 03.01.05, 03.01.06, and 03.01.07.   | Functional     | No Relationship   | N/A  | N/A      | N/A  | 0                        | No applicable SCF control   |
| 03.13.04   | Information in Shared System Resources                       | Prevent unauthorized and unintended information transfer via shared system resources.  | Functional     | Equal             | Information in Shared Resources                                | SEA-05   | Mechanisms exist to prevent unauthorized and unintended information transfer via shared system resources.  | 10                       |   |
| 03.13.05   | Withdrawn  | Incorporated into 03.13.01.  | Functional     | No Relationship   | N/A  | N/A      | N/A  | 0                        | No applicable SCF control   |
| 03.13.06   | Network Communications: Deny by Default - Allow by Exception | Deny network communications traffic by default, and allow network communications traffic by exception.   | Functional     | Equal             | 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).  | 10                       |   |
| 03.13.07   | Withdrawn  | Addressed by 03.01.12, 03.04.02 and 03.04.06.  | Functional     | No Relationship   | N/A  | N/A      | N/A  | 0                        | No applicable SCF control   |
| 03.13.08   | Transmission and Storage: Confidentiality                    | Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during transmission and while in storage.   | Functional     | Subset Of         | Use of Cryptographic Controls                                  | CRY-01   | Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.   | 10                       |   |
| 03.13.08   | Transmission and Storage: Confidentiality                    | Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during transmission and while in storage.   | 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                        |   |
| 03.13.08   | Transmission and Storage: Confidentiality                    | Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during transmission and while in storage.   | Functional     | Intersects With   | Transmission Confidentiality                                   | CRY-03   | Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.   | 5                        |   |
| 03.13.08   | Transmission and Storage: Confidentiality                    | Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during transmission and while in storage.   | Functional     | Intersects With   | Encrypting Data At Rest  | CRY-05   | Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.   | 5                        |   |
| 03.13.08   | Transmission and Storage: Confidentiality                    | Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during transmission and while in storage.   | Functional     | Intersects With   | Storage Media  | CRY-05.1 | Cryptographic mechanisms exist to protect the confidentiality and integrity of sensitive/regulated data residing on storage media.   | 5                        |   |
| 03.13.09   | Network Disconnect   | Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.   | Functional     | Equal             | Network Connection Termination                                 | NET-07   | Mechanisms exist to terminate network connections at the end of a session or after an organization-defined time period of inactivity.  | 10                       | ODP Value: no longer than 15 minutes  |
| 03.13.10   | Cryptographic Key Establishment and Management               | Establish and manage cryptographic keys in the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].  | Functional     | Intersects With   | Public Key Infrastructure (PKI)                                | CRY-08   | Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.  | 8                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.13.10   | Cryptographic Key Establishment and Management               | Establish and manage cryptographic keys in the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].  | Functional     | Subset Of         | Cryptographic Key Management                                   | CRY-09   | Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.   | 10                       | ODP Value: Guidance: At a minimum, establish a policy and procedure in line with the latest Cryptographic key management guidance.  |
| 03.13.10   | Cryptographic Key Establishment and Management               | Establish and manage cryptographic keys in the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].  | Functional     | Intersects With   | Cryptographic Key Loss or Change                               | CRY-09.3 | Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.   | 8                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.13.10   | Cryptographic Key Establishment and Management               | Establish and manage cryptographic keys in the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].  | Functional     | Intersects With   | Control & Distribution of Cryptographic Keys                   | CRY-09.4 | Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.   | 8                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.13.11   | Cryptographic Protection                                     | Implement the following types of cryptography to protect the confidentiality of CUI: [Assignment: organization-defined types of cryptography].   | Functional     | Intersects With   | 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. | 3                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.13.11   | Cryptographic Protection                                     | Implement the following types of cryptography to protect the confidentiality of CUI: [Assignment: organization-defined types of cryptography].   | Functional     | Subset Of         | Use of Cryptographic Controls                                  | CRY-01   | Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.   | 10                       | ODP Value: FIPS Validated Cryptography (https://csrc.nist.gov/Projects/Cryptographic-Module/Validated-Modules)  |
| 03.13.11   | Cryptographic Protection                                     | Implement the following types of cryptography to protect the confidentiality of CUI: [Assignment: organization-defined types of cryptography].   | Functional     | Intersects With   | Cryptographic Cipher Suites and Protocols Inventory            | CRY-01.5 | Mechanisms exist to identify, document and review deployed cryptographic cipher suites and protocols to proactively respond to industry trends regarding the continued viability of utilized cryptographic cipher suites and protocols.  | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.13.12   | Collaborative Computing Devices and Applications             | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A  | 0                        | No applicable SCF control   |
| 03.13.12.a | Collaborative Computing Devices and Applications             | Prohibit the remote activation of collaborative computing devices and applications with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed].  | 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) Video teleconferencing cameras; and (2) Video teleconferencing cameras; and (3) Teleconferencing microphones.   | 10                       | ODP Value: only as enumerated and justified in the System Security Plan before such remote activation occurs, and only when there are no other options, and the remote activation is operationally critical |
| 03.13.12.b | Collaborative Computing Devices and Applications             | Provide an explicit indication of use to users physically present at the devices.  | 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  |
|---------------|--|--|----------------|-------------------|--|----------|---|--------------------------|--|
| 03.13.12.b    | Collaborative Computing Devices and Applications | Provide an explicit indication of use to users physically present at the devices.  | Functional     | Equal             | Explicit Indication of Use                                       | END-14.6 | Mechanisms exist to configure collaborative computing devices to provide physically-present individuals with an explicit indication of use.   | 10                       |  |
| 03.13.13      | Mobile Code                                      | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.13.13.a    | Mobile Code                                      | Define acceptable mobile code and mobile code technologies.  | Functional     | Intersects With   | Explicitly Allow / Deny Applications                             | CFG-03.3 | Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.  | 8                        |  |
| 03.13.13.a    | Mobile Code                                      | Define acceptable mobile code and mobile code technologies.  | Functional     | Subset Of         | Mobile Code  | END-10   | Mechanisms exist to address mobile code / operating system-independent applications.  | 10                       |  |
| 03.13.13.b    | Mobile Code                                      | Authorize, monitor, and control the use of mobile code.  | 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                       |  |
| 03.13.13.b    | Mobile Code                                      | Authorize, monitor, and control the use of mobile code.  | Functional     | Intersects With   | Software Usage Restrictions                                      | CFG-04   | Mechanisms exist to enforce software usage restrictions to comply with applicable contract agreements and copyright laws.   | 3                        |  |
| 03.13.13.b    | Mobile Code                                      | Authorize, monitor, and control the use of mobile code.  | Functional     | Intersects With   | Open Source Software   | CFG-04.1 | Mechanisms exist to establish parameters for the secure use of open source software.  | 3                        |  |
| 03.13.13.b    | Mobile Code                                      | Authorize, monitor, and control the use of mobile code.  | Functional     | Intersects With   | User-Installed Software  | CFG-05   | Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.  | 3                        |  |
| 03.13.13.b    | Mobile Code                                      | Authorize, monitor, and control the use of mobile code.  | Functional     | Subset Of         | Mobile Code  | END-10   | Mechanisms exist to address mobile code / operating system-independent applications.  | 10                       |  |
| 03.13.14      | Withdrawn  | Technology-specific.   | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.13.15      | Session Authenticity                             | Protect the authenticity of communications sessions.   | Functional     | Subset Of         | Session Integrity  | NET-09   | Mechanisms exist to protect the authenticity and integrity of communications sessions.  | 10                       |  |
| 03.13.16      | Withdrawn  | Incorporated into 03.13.08.  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.14.01      | Flaw Remediation                                 | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.14.01.a    | Flaw Remediation                                 | Identify, report, and correct system flaws.  | Functional     | Intersects With   | Capabilities Deficiency Tracking                                 | IAO-05   | (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., ass/process owner);  | 5                        |  |
| 03.14.01.a    | Flaw Remediation                                 | Identify, report, and correct system flaws.  | Functional     | Intersects With   | Technology Development & Acquisition                             | TDA-01   | Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.   | 8                        |  |
| 03.14.01.a    | Flaw Remediation                                 | Identify, report, and correct system flaws.  | Functional     | Intersects With   | 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. | 8                        |  |
| 03.14.01.a    | Flaw Remediation                                 | Identify, report, and correct 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                       |  |
| 03.14.01.a    | Flaw Remediation                                 | Identify, report, and correct system flaws.  | Functional     | Intersects With   | Attack Surface Scope   | VPM-01.1 | Mechanisms exist to define and manage the scope for its attack surface management activities.   | 5                        |  |
| 03.14.01.a    | Flaw Remediation                                 | Identify, report, and correct system flaws.  | Functional     | Intersects With   | Vulnerability Remediation Process                                | VPM-02   | Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.  | 8                        |  |
| 03.14.01.a    | Flaw Remediation                                 | Identify, report, and correct system flaws.  | Functional     | Intersects With   | Continuous Vulnerability Remediation Activities                  | VPM-04   | Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.  | 8                        |  |
| 03.14.01.a    | Flaw Remediation                                 | Identify, report, and correct system flaws.  | 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.  | 8                        |  |
| 03.14.01.b    | Flaw Remediation                                 | Install security-relevant software and firmware updates within Assignment: organization-defined time period) of the release of the updates.  | Functional     | Intersects With   | Continuous Vulnerability Remediation Activities                  | VPM-04   | Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.  | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.14.01.b    | Flaw Remediation                                 | Install security-relevant software and firmware updates within Assignment: organization-defined time period) of the release of the updates.  | 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.  | 8                        | ODP Value: thirty (30) days for high-risk flaws (including both critical and high), 90 days for moderate-risk flaws, and 180 days for low-risk flaws |
| 03.14.02      | Malicious Code Protection                        | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.14.02.a    | Malicious Code Protection                        | Implement malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.   | Functional     | Subset Of         | Endpoint Device Management (EDM)                                 | END-01   | Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.   | 10                       |  |
| 03.14.02.a    | Malicious Code Protection                        | Implement malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.   | Functional     | Subset Of         | Centralized Management of Antimalware Technologies               | END-04.3 | Mechanisms exist to centrally-manage antimalware technologies.  | 10                       |  |
| 03.14.02.a    | Malicious Code Protection                        | Implement malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.   | Functional     | Intersects With   | Always On Protection   | END-04.7 | Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.  | 5                        |  |
| 03.14.02.b    | Malicious Code Protection                        | Update malicious code protection mechanisms as new releases are available in accordance with configuration management policies and procedures.   | Functional     | Equal             | Automatic Antimalware Signature Updates                          | END-04.1 | Automated mechanisms exist to update antimalware technologies, including signature definitions.   | 10                       |  |
| 03.14.02.c    | Malicious Code Protection                        | Configure malicious code protection mechanisms to:   | Functional     | Intersects With   | Malicious Code Protection (Anti-Malware)                         | END-04   | Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.  | 5                        |  |
| 03.14.02.c.01 | Malicious Code Protection                        | Perform scans of the system (Assignment: organization-defined frequency) and real-time scans of files from external sources at endpoints or system entry and exit points as the files are downloaded, opened, or executed; and | Functional     | Intersects With   | Malicious Code Protection (Anti-Malware)                         | END-04   | Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.  | 8                        | ODP Value: at least weekly   |
| 03.14.02.c.01 | Malicious Code Protection                        | Perform scans of the system (Assignment: organization-defined frequency) and real-time scans of files from external sources at endpoints or system entry and exit points as the files are downloaded, opened, or executed; and | Functional     | Intersects With   | Always On Protection   | END-04.7 | Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.  | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.14.02.c.02 | Malicious Code Protection                        | Block malicious code, quarantine malicious code, or take other mitigation actions in response to malicious code detection.   | Functional     | Intersects With   | Malicious Code Protection (Anti-Malware)                         | END-04   | Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.  | 8                        |  |
| 03.14.02.c.02 | Malicious Code Protection                        | Block malicious code, quarantine malicious code, or take other mitigation actions in response to malicious code detection.   | Functional     | Intersects With   | Always On Protection   | END-04.7 | Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.  | 8                        |  |
| 03.14.03      | Security Alerts, Advisories, and Directives      | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.14.03.a    | Security Alerts, Advisories, and Directives      | Receive system security alerts, advisories, and directives from external organizations on an ongoing basis.  | Functional     | Subset Of         | 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 architecture, selection of security solutions, monitoring, threat hunting, response and recovery activities.  | 10                       |  |
| 03.14.03.a    | Security Alerts, Advisories, and Directives      | Receive system security alerts, advisories, and directives from external organizations on an ongoing basis.  | Functional     | Intersects With   | Threat Intelligence Feeds  | THR-03   | Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.   | 5                        |  |
| 03.14.03.b    | Security Alerts, Advisories, and Directives      | Generate and disseminate internal system security alerts, advisories, and directives, as necessary.  | Functional     | Intersects With   | Threat Analysis  | THR-10   | Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.  | 5                        |  |
| 03.14.03.b    | Security Alerts, Advisories, and Directives      | Generate and disseminate internal system security alerts, advisories, and directives, as necessary.  | Functional     | Intersects With   | Impact-Level Prioritization                                      | RSK-02.1 | Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.  | 5                        |  |
| 03.14.03.b    | Security Alerts, Advisories, and Directives      | Generate and disseminate internal system security alerts, advisories, and directives, as necessary.  | Functional     | Equal             | Threat Intelligence Reporting                                    | THR-03.1 | Mechanisms exist to utilize external threat intelligence feeds to generate and disseminate organization-specific security alerts, advisories and directives.  | 10                       |  |
| 03.14.04      | Withdrawn  | Incorporated into 03.14.02.  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.14.05      | Withdrawn  | Addressed by 03.14.02.   | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.14.06      | System Monitoring                                | N/A  | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.14.06.a    | System Monitoring                                | Monitor the system to detect:  | Functional     | Subset Of         | Continuous Monitoring  | MON-01   | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.   | 10                       |  |
| 03.14.06.a.01 | System Monitoring                                | Attacks and indicators of potential attacks and  | Functional     | Intersects With   | Host Intrusion Detection and Prevention Systems (HIDS / HIPS)    | END-07   | Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS), or similar technologies, to monitor for and protect against anomalous host activity, including lateral movement across the network.  | 8                        |  |
| 03.14.06.a.01 | System Monitoring                                | Attacks and indicators of potential attacks and  | Functional     | Intersects With   | 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.   | 8                        |  |
| 03.14.06.a.01 | System Monitoring                                | Attacks and indicators of potential attacks and  | Functional     | Intersects With   | Monitoring for Indicators of Compromise (IOC)                    | MON-11.3 | Automated mechanisms exist to identify and alert on Indicators of Compromise (IOC).   | 8                        |  |
| 03.14.06.a.01 | System Monitoring                                | Attacks and indicators of potential attacks and  | Functional     | Intersects With   | Anomalous Behavior   | MON-16   | Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.   | 8                        |  |
| 03.14.06.a.02 | System Monitoring                                | Unauthorized connections.  | Functional     | Intersects With   | Host Intrusion Detection and Prevention Systems (HIDS / HIPS)    | END-07   | Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS), or similar technologies, to monitor for and protect against anomalous host activity, including lateral movement across the network.  | 8                        |  |
| 03.14.06.a.02 | System Monitoring                                | Unauthorized connections.  | Functional     | Intersects With   | Monitoring for Indicators of Compromise (IOC)                    | MON-11.3 | Automated mechanisms exist to identify and alert on Indicators of Compromise (IOC).   | 8                        |  |
| 03.14.06.a.02 | System Monitoring                                | Unauthorized connections.  | Functional     | Intersects With   | Anomalous Behavior   | MON-16   | Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.   | 8                        |  |
| 03.14.06.b    | System Monitoring                                | Identify unauthorized use of the system.   | Functional     | Intersects With   | Host Intrusion Detection and Prevention Systems (HIDS / HIPS)    | END-07   | Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS), or similar technologies, to monitor for and protect against anomalous host activity, including lateral movement across the network.  | 8                        |  |
| 03.14.06.b    | System Monitoring                                | Identify unauthorized use of the system.   | Functional     | Intersects With   | 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.   | 8                        |  |
| 03.14.06.b    | System Monitoring                                | Identify unauthorized use of the system.   | Functional     | Intersects With   | Monitoring for Indicators of Compromise (IOC)                    | MON-11.3 | Automated mechanisms exist to identify and alert on Indicators of Compromise (IOC).   | 8                        |  |
| 03.14.06.b    | System Monitoring                                | Identify unauthorized use of the system.   | Functional     | Intersects With   | Anomalous Behavior   | MON-16   | Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.   | 8                        |  |
| 03.14.06.c    | System Monitoring                                | Monitor inbound and outbound communications traffic to detect unusual or unauthorized activities or conditions.  | Functional     | Intersects With   | Host Intrusion Detection and Prevention Systems (HIDS / HIPS)    | END-07   | Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS), or similar technologies, to monitor for and protect against anomalous host activity, including lateral movement across the network.  | 8                        |  |
| 03.14.06.c    | System Monitoring                                | Monitor inbound and outbound communications traffic to detect unusual or unauthorized activities or conditions.  | Functional     | Intersects With   | Inbound & Outbound Communications Traffic                        | MON-01.3 | Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.  | 8                        |  |

| 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  |
|---------------|--------------------------------------|--|----------------|-------------------|---|----------|---|--------------------------|--|
| 03.14.06.c    | System Monitoring                    | Monitor inbound and outbound communications traffic to detect unusual or unauthorized activities or conditions.  | Functional     | Intersects With   | 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.   | 8                        |  |
| 03.14.06.c    | System Monitoring                    | Monitor inbound and outbound communications traffic to detect unusual or unauthorized activities or conditions.  | Functional     | Intersects With   | Monitoring for Indicators of Compromise (IOC)                         | MON-11.3 | Automated mechanisms exist to identify and alert on Indicators of Compromise (IOC).   | 8                        |  |
| 03.14.06.c    | System Monitoring                    | Monitor inbound and outbound communications traffic to detect unusual or unauthorized activities or conditions.  | Functional     | Intersects With   | Anomalous Behavior  | MON-16   | Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.   | 8                        |  |
| 03.14.06.c    | System Monitoring                    | Monitor inbound and outbound communications traffic to detect unusual or unauthorized activities or conditions.  | Functional     | Intersects With   | Network Intrusion Detection / Prevention Systems (NIDS / NIPS)        | NET-08   | Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.   | 8                        |  |
| 03.14.06.c    | System Monitoring                    | Monitor inbound and outbound communications traffic to detect unusual or unauthorized activities or conditions.  | 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.  | 8                        |  |
| 03.14.07      | Withdraw                             | Incorporated into 03.14.06.  | Functional     | No Relationship   | N/A   | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.14.08      | Information Management and Retention | Manage and retain CUI within the system and CUI output from the system in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements. | 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                       |  |
| 03.15.01      | Policy and Procedures                | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.15.01.a    | Policy and Procedures                | Develop, document, and disseminate to organizational personnel or roles the policies and procedures needed to satisfy the security requirements for the protection of CUI.   | Functional     | Subset Of         | Security, Compliance & Resilience Program (SCRP)                      | GOV-01   | Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.   | 10                       |  |
| 03.15.01.a    | Policy and Procedures                | Develop, document, and disseminate to organizational personnel or roles the policies and procedures needed to satisfy the security requirements for the protection of CUI.   | Functional     | Equal             | 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                       |  |
| 03.15.01.a    | Policy and Procedures                | Develop, document, and disseminate to organizational personnel or roles the policies and procedures needed to satisfy the security requirements for the protection of CUI.   | Functional     | Intersects With   | Operationalizing Security, Compliance & Resilience Capabilities       | GOV-15   | Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.   | 8                        |  |
| 03.15.01.a    | Policy and Procedures                | Develop, document, and disseminate to organizational personnel or roles the policies and procedures needed to satisfy the security requirements for the protection of CUI.   | Functional     | Intersects With   | Select Controls   | GOV-15.1 | Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.   | 8                        |  |
| 03.15.01.a    | Policy and Procedures                | Develop, document, and disseminate to organizational personnel or roles the policies and procedures needed to satisfy the security requirements for the protection of CUI.   | Functional     | Intersects With   | Implement Controls  | GOV-15.2 | Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.  | 8                        |  |
| 03.15.01.a    | Policy and Procedures                | Develop, document, and disseminate to organizational personnel or roles the policies and procedures needed to satisfy the security requirements for the protection of CUI.   | Functional     | Intersects With   | Assess Controls   | GOV-15.3 | Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control are:<br>(1) Implemented correctly; and<br>(2) Operating as intended.  | 8                        |  |
| 03.15.01.a    | Policy and Procedures                | Develop, document, and disseminate to organizational personnel or roles the policies and procedures needed to satisfy the security requirements for the protection of CUI.   | Functional     | Intersects With   | Authorize Technology Assets, Applications and/or Services (TAAS)      | GOV-15.4 | Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control.   | 8                        |  |
| 03.15.01.a    | Policy and Procedures                | Develop, document, and disseminate to organizational personnel or roles the policies and procedures needed to satisfy the security requirements for the protection of CUI.   | Functional     | Intersects With   | Monitor Controls  | GOV-15.5 | Mechanisms exist to compel data and/or process owners to monitor Technology Assets, Applications, Services and/or Data (TAASD) under their control on an ongoing basis for applicable threats and risks, as well as to ensure security, compliance and resilience controls are operating as intended.   | 8                        |  |
| 03.15.01.a    | Policy and Procedures                | Develop, document, and disseminate to organizational personnel or roles the policies and procedures needed to satisfy the security requirements for the protection of CUI.   | Functional     | Intersects With   | Operations Security   | OPS-01   | Mechanisms exist to facilitate the implementation of operational security controls.   | 8                        |  |
| 03.15.01.a    | Policy and Procedures                | Develop, document, and disseminate to organizational personnel or roles the policies and procedures needed to satisfy the security requirements for the protection of CUI.   | Functional     | Intersects With   | 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.   | 8                        |  |
| 03.15.01.b    | Policy and Procedures                | Review and update policies and procedures [Assignment: organization-defined frequency].  | Functional     | Subset Of         | 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.   | 10                       | ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks |
| 03.15.01.b    | Policy and Procedures                | Review and update policies and procedures [Assignment: organization-defined frequency].  | Functional     | Intersects With   | Operations Security   | OPS-01   | Mechanisms exist to facilitate the implementation of operational security controls.   | 3                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.15.01.b    | Policy and Procedures                | Review and update policies and procedures [Assignment: organization-defined frequency].  | 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 required standards to achieve the specific goals of the process area.  | 3                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.15.02      | System Security Plan                 | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.15.02.a    | System Security Plan                 | Develop a system security plan that:   | Functional     | Subset Of         | Applied Security, Compliance and Resilience Controls Documentation    | IAO-03   | Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPITDF) that are contained within the system. | 10                       | changes  |
| 03.15.02.a.01 | System Security Plan                 | Defines the constituent system components;   | Functional     | Subset Of         | Applied Security, Compliance and Resilience Controls Documentation    | IAO-03   | Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPITDF) that are contained within the system. | 10                       |  |
| 03.15.02.a.02 | System Security Plan                 | Identifies the information types processed, stored, and transmitted by the system;   | Functional     | Subset Of         | Applied Security, Compliance and Resilience Controls Documentation    | IAO-03   | Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPITDF) that are contained within the system. | 10                       |  |
| 03.15.02.a.03 | System Security Plan                 | Describes specific threats to the system that are of concern to the organization;  | Functional     | Subset Of         | Applied Security, Compliance and Resilience Controls Documentation    | IAO-03   | Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPITDF) that are contained within the system. | 10                       |  |
| 03.15.02.a.03 | System Security Plan                 | Describes specific threats to the system that are of concern to the organization;  | Functional     | Intersects With   | Risk Catalog  | RSK-03.1 | Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.  | 3                        |  |
| 03.15.02.a.03 | System Security Plan                 | Describes specific threats to the system that are of concern to the organization;  | Functional     | Intersects With   | Threat Catalog  | THR-09   | Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.   | 8                        |  |
| 03.15.02.a.04 | System Security Plan                 | Describes the operational environment for the system and any dependencies on or connections to other systems or system components;   | Functional     | Intersects With   | Control Applicability Boundary Graphical Representation               | AST-04.2 | Mechanisms exist to ensure control applicability is appropriately-determined for Technology Assets, Applications and/or Services (TAAS) and third parties by graphically representing applicable boundaries.  | 8                        |  |
| 03.15.02.a.04 | System Security Plan                 | Describes the operational environment for the system and any dependencies on or connections to other systems or system components;   | Functional     | Intersects With   | Compliance Scope  | CPL-01.2 | Mechanisms exist to document and validate the scope of security, compliance and resilience controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.  | 8                        |  |
| 03.15.02.a.04 | System Security Plan                 | Describes the operational environment for the system and any dependencies on or connections to other systems or system components;   | Functional     | Subset Of         | Applied Security, Compliance and Resilience Controls Documentation    | IAO-03   | Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPITDF) that are contained within the system. | 10                       |  |
| 03.15.02.a.05 | System Security Plan                 | Provides an overview of the security requirements for the system;  | Functional     | Subset Of         | Applied Security, Compliance and Resilience Controls Documentation    | IAO-03   | Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPITDF) that are contained within the system. | 10                       |  |
| 03.15.02.a.06 | System Security Plan                 | Describes the safeguards in place or planned for meeting the security requirements;  | Functional     | Subset Of         | Applied Security, Compliance and Resilience Controls Documentation    | IAO-03   | Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPITDF) that are contained within the system. | 10                       |  |
| 03.15.02.a.07 | System Security Plan                 | Identifies individuals that fulfill system roles and responsibilities; and   | Functional     | Subset Of         | Applied Security, Compliance and Resilience Controls Documentation    | IAO-03   | Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPITDF) that are contained within the system. | 10                       |  |
| 03.15.02.a.08 | System Security Plan                 | Includes other relevant information necessary for the protection of CUI.   | Functional     | Subset Of         | Applied Security, Compliance and Resilience Controls Documentation    | IAO-03   | Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPITDF) that are contained within the system. | 10                       |  |
| 03.15.02.b    | System Security Plan                 | Review and update the system security plan [Assignment: organization-defined frequency].   | Functional     | Subset Of         | Applied Security, Compliance and Resilience Controls Documentation    | IAO-03   | Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPITDF) that are contained within the system. | 10                       | ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks |
| 03.15.02.c    | System Security Plan                 | Protect the system security plan from unauthorized disclosure.   | Functional     | Intersects With   | Defining Access Authorizations for Sensitive / Regulated Data         | DCH-01.4 | Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and/or physical access to sensitive/regulated data.  | 8                        |  |
| 03.15.02.c    | System Security Plan                 | Protect the system security plan from unauthorized disclosure.   | Functional     | Intersects With   | Disclosure of Information   | DCH-03.1 | Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.  | 8                        |  |
| 03.15.03      | Rules of Behavior                    | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.15.03.a    | Rules of Behavior                    | Establish rules that describe the responsibilities and expected behavior for system usage and protecting CUI.  | Functional     | Subset Of         | Human Resources Security Management                                   | HRS-01   | Mechanisms exist to facilitate the implementation of personnel security controls.   | 10                       |  |
| 03.15.03.a    | Rules of Behavior                    | Establish rules that describe the responsibilities and expected behavior for system usage and protecting CUI.  | Functional     | Intersects With   | Terms of Employment   | HRS-05   | Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.   | 10                       |  |
| 03.15.03.a    | Rules of Behavior                    | Establish rules that describe the responsibilities and expected behavior for system usage and protecting CUI.  | Functional     | Subset Of         | Rules of Behavior   | HRS-05.1 | Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.   | 10                       |  |
| 03.15.03.a    | Rules of Behavior                    | Establish rules that describe the responsibilities and expected behavior for system usage and protecting CUI.  | Functional     | Intersects With   | Social Media & Social Networking Restrictions                         | HRS-05.2 | Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.  | 10                       |  |

| 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  |
|------------|---------------------------------|--|----------------|-------------------|---|----------|--|--------------------------|--|
| 03.15.03.a | Rules of Behavior               | Establish rules that describe the responsibilities and expected behavior for system usage and protecting CUI.  | Functional     | Intersects With   | Technology Use Restrictions   | HR5-03   | Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.  | 8                        |  |
| 03.15.03.a | Rules of Behavior               | Establish rules that describe the responsibilities and expected behavior for system usage and protecting CUI.  | Functional     | Intersects With   | Use of Critical Technologies  | HR5-04   | Mechanisms exist to govern usage policies for critical technologies.   | 8                        |  |
| 03.15.03.a | Rules of Behavior               | Establish rules that describe the responsibilities and expected behavior for system usage and protecting CUI.  | Functional     | Intersects With   | Use of Mobile Devices   | HR5-05   | Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.   | 8                        |  |
| 03.15.03.b | Rules of Behavior               | Provide rules to individuals who require access to the system.   | Functional     | Intersects With   | Defined Roles & Responsibilities                                      | HR5-03   | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.   | 8                        |  |
| 03.15.03.b | Rules of Behavior               | Provide rules to individuals who require access to the system.   | Functional     | Intersects With   | User Awareness  | HR5-03.1 | Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.   | 8                        |  |
| 03.15.03.b | Rules of Behavior               | Provide rules to individuals who require access to the system.   | Functional     | Intersects With   | Formal Indoctrination   | HR5-04.2 | Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access.  | 8                        |  |
| 03.15.03.b | Rules of Behavior               | Provide rules to individuals who require access to the system.   | Functional     | Intersects With   | Policy Familiarization & Acknowledgement                              | HR5-05.7 | Mechanisms exist to ensure personnel receive recurring familiarization with the organization's security, compliance and resilience policies and provide acknowledgement.   | 8                        |  |
| 03.15.03.b | Rules of Behavior               | Provide rules to individuals who require access to the system.   | Functional     | Intersects With   | Access Agreements   | HR5-06   | Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.  | 8                        |  |
| 03.15.03.c | Rules of Behavior               | Receive a documented acknowledgement from individuals indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to CUI and the system.                           | Functional     | Intersects With   | Policy Familiarization & Acknowledgement                              | HR5-05.7 | Mechanisms exist to ensure personnel receive recurring familiarization with the organization's security, compliance and resilience policies and provide acknowledgement.   | 8                        |  |
| 03.15.03.c | Rules of Behavior               | Receive a documented acknowledgement from individuals indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to CUI and the system.                           | Functional     | Intersects With   | Access Agreements   | HR5-06   | Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.  | 8                        |  |
| 03.15.03.c | Rules of Behavior               | Receive a documented acknowledgement from individuals indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to CUI and the system.                           | Functional     | Intersects With   | Confidentiality Agreements  | HR5-06.1 | 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.  | 3                        |  |
| 03.15.03.d | Rules of Behavior               | Review and update the rules of behavior [Assignment: organization-defined frequency].  | 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.  | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.15.03.d | Rules of Behavior               | Review and update the rules of behavior [Assignment: organization-defined frequency].  | Functional     | Subset Of         | Human Resources Security Management                                   | HR5-01   | Mechanisms exist to facilitate the implementation of personnel security controls.  | 10                       | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.15.03.d | Rules of Behavior               | Review and update the rules of behavior [Assignment: organization-defined frequency].  | Functional     | Equal             | Rules of Behavior   | HR5-05.1 | Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.  | 10                       | ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks   |
| 03.15.03.d | Rules of Behavior               | Review and update the rules of behavior [Assignment: organization-defined frequency].  | Functional     | Intersects With   | Policy Familiarization & Acknowledgement                              | HR5-05.7 | Mechanisms exist to ensure personnel receive recurring familiarization with the organization's security, compliance and resilience policies and provide acknowledgement.   | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.16.01   | Security Engineering Principles | Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization-defined systems security engineering principles].          | Functional     | Intersects With   | Prohibited Equipment & Services                                       | AST-17   | Mechanisms exist to govern Supply Chain Risk Management (SCRM) sanctions that require the removal and prohibition of certain Technology Assets, Applications and/or Services (TAAS) that are designated as supply chain threats by a statutory or regulatory body.   | 3                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.16.01   | Security Engineering Principles | Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization-defined systems security engineering principles].          | Functional     | Intersects With   | 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.  | 3                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.16.01   | Security Engineering Principles | Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization-defined systems security engineering principles].          | Functional     | Intersects With   | Security, Compliance & Resilience Requirements Definition             | PRM-05   | Mechanisms exist to identify critical system components and functions by performing a critically analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).  | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.16.01   | Security Engineering Principles | Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization-defined systems security engineering principles].          | 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                       | ODP Value: Guidance: At a minimum, documentation that provides user and administrator guidance for the implementation and operation of controls. The level of detail required in such documentation should be based on the degree to which organizations depend on the capabilities, functions, or mechanisms to meet risk response expectations. Requirements can include mandated configuration settings that specify allowed functions, ports, protocols, and services. Acceptance criteria for systems, system components, and system services are defined in the same manner as the criteria for any organizational acquisition or procurement. |
| 03.16.01   | Security Engineering Principles | Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization-defined systems security engineering principles].          | 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.   | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.16.01   | Security Engineering Principles | Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization-defined systems security engineering principles].          | Functional     | Intersects With   | Technology Development & Acquisition                                  | TDA-01   | Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.  | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.16.01   | Security Engineering Principles | Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization-defined systems security engineering principles].          | 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                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.16.01   | Security Engineering Principles | Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization-defined systems security engineering principles].          | Functional     | Intersects With   | Development Methods, Techniques & Processes                           | TDA-02.3 | Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure development practices, such as pre-established, secure configuration implemented, and (2) use the pre-established, secure configuration as the default for any subsequent TAAS reinstallation or upgrade.  | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.16.01   | Security Engineering Principles | Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization-defined systems security engineering principles].          | Functional     | Intersects With   | Pre-Established Secure Configurations                                 | TDA-02.4 | Mechanisms exist to ensure vendors / manufacturers: (1) Deliver the Technology Asset, Application and/or Service (TAAS) with a pre-established, secure configuration implemented; and (2) Use the pre-established, secure configuration as the default for any subsequent TAAS reinstallation or upgrade.  | 3                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.16.01   | Security Engineering Principles | Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization-defined systems security engineering principles].          | Functional     | Intersects With   | Commercial Off-the-Shelf (COTS) Security Solutions                    | TDA-03   | Mechanisms exist to utilize only Commercial Off-the-Shelf (COTS) security products.  | 3                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.16.01   | Security Engineering Principles | Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization-defined systems security engineering principles].          | Functional     | Intersects With   | Developer Architecture & Design                                       | TDA-05   | Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a design specification and security architecture that: (1) is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; (2) Accuracy and completeness describes the required security functionality and the location of security, compliance and resilience controls among physical and logical components; and (3) Expresses how individual security functions, mechanisms and services work together to provide required security capabilities and a unified approach to protection. | 5                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.16.01   | Security Engineering Principles | Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization-defined systems security engineering principles].          | Functional     | Intersects With   | Secure Software Development Practices (SSDP)                          | TDA-06   | Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).  | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.16.01   | Security Engineering Principles | Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization-defined systems security engineering principles].          | Functional     | Intersects With   | Third-Party Management  | TPM-01   | Mechanisms exist to facilitate the implementation of third-party management controls.  | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.16.01   | Security Engineering Principles | Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization-defined systems security engineering principles].          | 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.  | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.16.02   | Unsupported System Components   | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control  |
| 03.16.02.a | Unsupported System Components   | Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.  | Functional     | Subset Of         | Technology Lifecycle Management                                       | SEA-07.1 | Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).  | 10                       |  |
| 03.16.02.a | Unsupported System Components   | Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.  | Functional     | Equal             | 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                       |  |
| 03.16.02.b | Unsupported System Components   | Provide options for risk mitigation or alternative sources for continued support for unsupported components that cannot be replaced.   | Functional     | Intersects With   | Predictable Failure Analysis  | SEA-07   | Mechanisms exist to determine the Mean Time to Failure (MTTF) for system components in specific environments of operation.   | 3                        |  |
| 03.16.02.b | Unsupported System Components   | Provide options for risk mitigation or alternative sources for continued support for unsupported components that cannot be replaced.   | Functional     | Intersects With   | Technology Lifecycle Management                                       | SEA-07.1 | Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).  | 8                        |  |
| 03.16.02.b | Unsupported System Components   | Provide options for risk mitigation or alternative sources for continued support for unsupported components that cannot be replaced.   | Functional     | Equal             | 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).   | 10                       |  |
| 03.16.03   | External System Services        | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A  | 0                        | No applicable SCF control  |
| 03.16.03.a | External System Services        | Require the providers of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements: [Assignment: organization-defined security requirements]. | Functional     | Subset Of         | Third-Party Management  | TPM-01   | Mechanisms exist to facilitate the implementation of third-party management controls.  | 10                       | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.16.03.a | External System Services        | Require the providers of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements: [Assignment: organization-defined security requirements]. | Functional     | Intersects With   | 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).   | 8                        | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.16.03.a | External System Services        | Require the providers of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements: [Assignment: organization-defined security requirements]. | 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.  | 8                        | DoD-provided ODP does not apply to this specific 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  |
|------------|--|---|----------------|-------------------|--|----------|---|--------------------------|--|
| 03.16.03.a | External System Services                   | Require the providers of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements: [Assignment: organization-defined security requirements].                            | Functional     | Intersects With   | 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).  | 8                        | ODP Values:<br>(1) For cloud service providers:<br>(i) FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline in accordance with the FedRAMP Marketplace; or<br>(ii) meets security requirements established by the government equivalent to the FedRAMP Moderate (or higher) baseline.<br>(2) All other external service providers must meet NIST SP 800-171 R2. |
| 03.16.03.a | External System Services                   | Require the providers of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements: [Assignment: organization-defined security requirements].                            | Functional     | Intersects With   | Contract Flow-Down Requirements  | TPM-05.2 | Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.  | 8                        | ODP Values:<br>(1) For cloud service providers:<br>(i) FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline in accordance with the FedRAMP Marketplace; or<br>(ii) meets security requirements established by the government equivalent to the FedRAMP Moderate (or higher) baseline.<br>(2) All other external service providers must meet NIST SP 800-171 R2. |
| 03.16.03.a | External System Services                   | Require the providers of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements: [Assignment: organization-defined security requirements].                            | Functional     | Equal             | Third-Party Attestation (SPA)  | TPM-05.8 | Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (TPAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.   | 10                       | DoD-provided ODP does not apply to this specific SCF control.  |
| 03.16.03.b | External System Services                   | Define and document user roles and responsibilities with regard to external system services, including shared responsibilities with external service providers.   | Functional     | Intersects With   | Defined Roles & Responsibilities   | HRS-03   | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.  | 8                        |  |
| 03.16.03.b | External System Services                   | Define and document user roles and responsibilities with regard to external system services, including shared responsibilities with external service providers.   | Functional     | Intersects With   | 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.   | 8                        |  |
| 03.16.03.b | External System Services                   | Define and document user roles and responsibilities with regard to external system services, including shared responsibilities with external service providers.   | Functional     | Intersects With   | 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).  | 5                        |  |
| 03.16.03.b | External System Services                   | Define and document user roles and responsibilities with regard to external system services, including shared responsibilities with external service providers.   | Functional     | Intersects With   | Contract Flow-Down Requirements  | TPM-05.2 | Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.  | 5                        |  |
| 03.16.03.b | External System Services                   | Define and document user roles and responsibilities with regard to external system services, including shared responsibilities with external service providers.   | Functional     | Equal             | Responsible, Accountable, Supportive, Consulted & Informed (RASC) Matrix | TPM-05.4 | Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASC) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).   | 10                       |  |
| 03.16.03.c | External System Services                   | Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.  | Functional     | Intersects With   | 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).  | 5                        |  |
| 03.16.03.c | External System Services                   | Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.  | Functional     | Intersects With   | 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).  | 5                        |  |
| 03.16.03.c | External System Services                   | Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.  | Functional     | Intersects With   | Contract Flow-Down Requirements  | TPM-05.2 | Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.<br>Accountable, Supportive, Consulted & Informed (RASC) matrix, or similar documentation, to ensure security, compliance and resilience control assignments accurately reflect current:<br>(1) Contractual obligations for the External Service Provider (ESP);<br>(2) Business practices;<br>(3) Applicable stakeholders; and<br>(4) Deployed Technology Assets, Applications and/or Services | 5                        |  |
| 03.16.03.c | External System Services                   | Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.  | Functional     | Intersects With   | Third-Party Scope Review   | TPM-05.5 | Mechanisms exist to obtain a First-Party Declaration (FPD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to subcontractors.   | 8                        |  |
| 03.16.03.c | External System Services                   | Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.  | Functional     | Intersects With   | First-Party Declaration (FPD)  | TPM-05.6 | Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (TPAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.   | 5                        |  |
| 03.16.03.c | External System Services                   | Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.  | Functional     | Intersects With   | Third-Party Attestation (SPA)  | TPM-05.8 | Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (TPAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.   | 8                        |  |
| 03.16.03.c | External System Services                   | Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.  | 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                       |  |
| 03.17.01   | Supply Chain Risk Management Plan          | N/A   | Functional     | No Relationship   | N/A  | N/A      | N/A   | 0                        | No applicable SCF control  |
| 03.17.01.a | Supply Chain Risk Management Plan          | Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. | Functional     | Intersects With   | Operationalizing Security, Compliance & Resilience Capabilities          | GOV-15   | Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.   | 3                        |  |
| 03.17.01.a | Supply Chain Risk Management Plan          | Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. | Functional     | Intersects With   | Select Controls  | GOV-15.1 | Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.   | 3                        |  |
| 03.17.01.a | Supply Chain Risk Management Plan          | Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. | Functional     | Intersects With   | Implement Controls   | GOV-15.2 | Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.  | 3                        |  |
| 03.17.01.a | Supply Chain Risk Management Plan          | Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. | Functional     | Intersects With   | Assess Controls  | GOV-15.3 | Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control are:<br>(1) Implemented correctly; and<br>(2) Operating as intended.  | 3                        |  |
| 03.17.01.a | Supply Chain Risk Management Plan          | Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. | Functional     | Intersects With   | Authorize Technology Assets, Applications and/or Services (TAAS)         | GOV-15.4 | Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control.   | 3                        |  |
| 03.17.01.a | Supply Chain Risk Management Plan          | Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. | Functional     | Intersects With   | Monitor Controls   | GOV-15.5 | Mechanisms exist to compel data and/or process owners to monitor Technology Assets, Applications, Services and/or Data (TAASD) under their control on an ongoing basis for applicable threats and risks, as well as to ensure security, compliance and resilience controls are operating as intended.   | 3                        |  |
| 03.17.01.a | Supply Chain Risk Management Plan          | Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. | Functional     | Subset Of         | Risk Management Program  | RSK-01   | Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.  | 10                       |  |
| 03.17.01.a | Supply Chain Risk Management Plan          | Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. | Functional     | Equal             | Supply Chain Risk Management (SCRM) Plan                                 | RSK-09   | Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.  | 10                       |  |
| 03.17.01.a | Supply Chain Risk Management Plan          | Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. | Functional     | Intersects With   | Supply Chain Risk Management (SCRM)                                      | TPM-03   | Mechanisms exist to:<br>(1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and<br>(2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.   | 8                        |  |
| 03.17.01.a | Supply Chain Risk Management Plan          | Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. | Functional     | Intersects With   | Acquisition Strategies, Tools & Methods                                  | TPM-03.1 | Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).  | 5                        |  |
| 03.17.01.a | Supply Chain Risk Management Plan          | Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services. | Functional     | Intersects With   | Break Clauses  | TPM-05.7 | Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.   | 3                        |  |
| 03.17.01.b | Supply Chain Risk Management Plan          | Review and update the supply chain risk management plan [Assignment: organization-defined frequency].   | Functional     | Subset Of         | Supply Chain Risk Management (SCRM) Plan                                 | RSK-09   | Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.  | 10                       | ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks   |
| 03.17.01.c | Supply Chain Risk Management Plan          | Protect the supply chain risk management plan from unauthorized disclosure.   | Functional     | Intersects With   | Sensitive / Regulated Data Protection                                    | DCH-01.2 | Mechanisms exist to protect sensitive/regulated data wherever it is produced and/or stored.   | 8                        |  |
| 03.17.01.c | Supply Chain Risk Management Plan          | Protect the supply chain risk management plan from unauthorized disclosure.   | Functional     | Intersects With   | Defining Access Authorizations for Sensitive / Regulated Data            | DCH-01.4 | Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and/or physical access to sensitive/regulated data.  | 8                        |  |
| 03.17.01.c | Supply Chain Risk Management Plan          | Protect the supply chain risk management plan from unauthorized disclosure.   | Functional     | Intersects With   | Disclosure of Information  | DCH-03.1 | Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.  | 8                        |  |
| 03.17.02   | Acquisition Strategies, Tools, and Methods | Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.  | 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                       |  |
| 03.17.02   | Acquisition Strategies, Tools, and Methods | Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.  | Functional     | Equal             | Acquisition Strategies, Tools & Methods                                  | TPM-03.1 | Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).  | 10                       |  |
| 03.17.02   | Acquisition Strategies, Tools, and Methods | Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.  | Functional     | Intersects With   | 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).  | 5                        |  |
| 03.17.02   | Acquisition Strategies, Tools, and Methods | Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.  | Functional     | Intersects With   | 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).   | 8                        |  |
| 03.17.02   | Acquisition Strategies, Tools, and Methods | Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.  | Functional     | Intersects With   | 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).  | 8                        |  |
| 03.17.02   | Acquisition Strategies, Tools, and Methods | Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.  | Functional     | Intersects With   | Security Compromise Notification Agreements                              | TPM-05.1 | Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.   | 3                        |  |
| 03.17.02   | Acquisition Strategies, Tools, and Methods | Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.  | Functional     | Intersects With   | Contract Flow-Down Requirements  | TPM-05.2 | Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.<br>Accountable, Supportive, Consulted & Informed (RASC) matrix, or similar documentation, to ensure security, compliance and resilience control assignments accurately reflect current:<br>(1) Contractual obligations for the External Service Provider (ESP);<br>(2) Business practices;<br>(3) Applicable stakeholders; and<br>(4) Deployed Technology Assets, Applications and/or Services | 8                        |  |
| 03.17.02   | Acquisition Strategies, Tools, and Methods | Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.  | Functional     | Intersects With   | Third-Party Scope Review   | TPM-05.5 | Mechanisms exist to obtain a First-Party Declaration (FPD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to subcontractors.   | 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   |
|------------|--|--|----------------|-------------------|---|----------|---|--------------------------|---|
| 03.17.02   | Acquisition Strategies, Tools, and Methods | Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.   | Functional     | Intersects With   | Break Clauses                                   | TPM-05.7 | Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.   | 5                        |   |
| 03.17.02   | Acquisition Strategies, Tools, and Methods | Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.   | Functional     | Intersects With   | Review of Third-Party Services                  | TPM-08   | Mechanisms exist to monitor, regularly review and assess External Service Providers (ESP) for compliance with established contractual requirements for security, compliance and resilience controls.  | 5                        |   |
| 03.17.02   | Acquisition Strategies, Tools, and Methods | Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.   | Functional     | Intersects With   | Third-Party Deficiency Remediation              | TPM-09   | Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.   | 5                        |   |
| 03.17.02   | Acquisition Strategies, Tools, and Methods | Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.   | 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                        |   |
| 03.17.03   | Supply Chain Requirements and Processes    | N/A  | Functional     | No Relationship   | N/A   | N/A      | N/A   | 0                        | No applicable SCF control   |
| 03.17.03.a | Supply Chain Requirements and Processes    | Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.  | Functional     | Subset Of         | Supply Chain Risk Management (SCRM) Plan        | RSK-09   | Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.  | 10                       |   |
| 03.17.03.a | Supply Chain Requirements and Processes    | Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.  | Functional     | Intersects With   | Supply Chain Risk Assessment                    | RSK-09.1 | Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).  | 8                        |   |
| 03.17.03.a | Supply Chain Requirements and Processes    | Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.  | Functional     | Intersects With   | Third-Party Criticality Assessments             | TPM-02   | Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.  | 8                        |   |
| 03.17.03.a | Supply Chain Requirements and Processes    | Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.  | Functional     | Intersects With   | Supply Chain Risk Management (SCRM)             | TPM-03   | Mechanisms exist to:<br>(1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and<br>(2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.   | 8                        |   |
| 03.17.03.a | Supply Chain Requirements and Processes    | Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.  | Functional     | Intersects With   | Acquisition Strategies, Tools & Methods         | TPM-03.1 | Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).  | 3                        |   |
| 03.17.03.a | Supply Chain Requirements and Processes    | Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.  | Functional     | Intersects With   | Limit Potential Harm                            | TPM-03.2 | Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.   | 3                        |   |
| 03.17.03.a | Supply Chain Requirements and Processes    | Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.  | Functional     | Intersects With   | Processes To Address Weaknesses or Deficiencies | TPM-03.3 | Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain.  | 5                        |   |
| 03.17.03.a | Supply Chain Requirements and Processes    | Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.  | Functional     | Intersects With   | 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).  | 5                        |   |
| 03.17.03.a | Supply Chain Requirements and Processes    | Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.  | Functional     | Intersects With   | 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).   | 5                        |   |
| 03.17.03.a | Supply Chain Requirements and Processes    | Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.  | Functional     | Intersects With   | Third-Party Scope Review                        | TPM-05.5 | Accountable, Supportive, Consulted & Informed (RASC) matrix, or similar documentation, to ensure security, compliance and resilience control assignments accurately reflect current:<br>(1) Contractual obligations for the External Service Provider (ESP);<br>(2) Business practices;<br>(3) Applicable stakeholders; and<br>(4) Deployed Technology Assets, Applications and/or Services | 5                        |   |
| 03.17.03.b | Supply Chain Requirements and Processes    | Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: (Assignment: organization-defined security requirements). | Functional     | Subset Of         | Supply Chain Risk Management (SCRM) Plan        | RSK-09   | Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.  | 10                       | ODP Value: at a minimum, integrate Supply Chain Risk Management (SCRM) into acquisition/procurement policies, provide adequate SCRM resources, define the SCRM control baseline, establish processes to ensure suppliers disclose significant vulnerabilities and significant incidents |
| 03.17.03.b | Supply Chain Requirements and Processes    | Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: (Assignment: organization-defined security requirements). | Functional     | Intersects With   | Supply Chain Risk Management (SCRM)             | TPM-03   | Mechanisms exist to:<br>(1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and<br>(2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.17.03.b | Supply Chain Requirements and Processes    | Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: (Assignment: organization-defined security requirements). | Functional     | Intersects With   | Acquisition Strategies, Tools & Methods         | TPM-03.1 | Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).  | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.17.03.b | Supply Chain Requirements and Processes    | Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: (Assignment: organization-defined security requirements). | Functional     | Intersects With   | Limit Potential Harm                            | TPM-03.2 | Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.17.03.b | Supply Chain Requirements and Processes    | Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: (Assignment: organization-defined security requirements). | Functional     | Intersects With   | Processes To Address Weaknesses or Deficiencies | TPM-03.3 | Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain.  | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.17.03.b | Supply Chain Requirements and Processes    | Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: (Assignment: organization-defined security requirements). | Functional     | Intersects With   | 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).  | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.17.03.b | Supply Chain Requirements and Processes    | Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: (Assignment: organization-defined security requirements). | Functional     | Intersects With   | 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).   | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.17.03.b | Supply Chain Requirements and Processes    | Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: (Assignment: organization-defined security requirements). | 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                       | ODP Value: at a minimum, integrate Supply Chain Risk Management (SCRM) into acquisition/procurement policies, provide adequate SCRM resources, define the SCRM control baseline, establish processes to ensure suppliers disclose significant vulnerabilities and significant incidents |
| 03.17.03.b | Supply Chain Requirements and Processes    | Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: (Assignment: organization-defined security requirements). | Functional     | Intersects With   | Contract Flow-Down Requirements                 | TPM-05.2 | Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.  | 8                        | ODP Value: at a minimum, integrate Supply Chain Risk Management (SCRM) into acquisition/procurement policies, provide adequate SCRM resources, define the SCRM control baseline, establish processes to ensure suppliers disclose significant vulnerabilities and significant incidents |
| 03.17.03.b | Supply Chain Requirements and Processes    | Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: (Assignment: organization-defined security requirements). | Functional     | Intersects With   | Third-Party Scope Review                        | TPM-05.5 | Accountable, Supportive, Consulted & Informed (RASC) matrix, or similar documentation, to ensure security, compliance and resilience control assignments accurately reflect current:<br>(1) Contractual obligations for the External Service Provider (ESP);<br>(2) Business practices;<br>(3) Applicable stakeholders; and<br>(4) Deployed Technology Assets, Applications and/or Services | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |
| 03.17.03.b | Supply Chain Requirements and Processes    | Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: (Assignment: organization-defined security requirements). | Functional     | Intersects With   | Break Clauses                                   | TPM-05.7 | Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.   | 5                        | DoD-provided ODP does not apply to this specific SCF control.   |