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

Focal Document: NIST SP 800-171A R3
Focal Document URL: https://csrc.nist.gov/pubs/sp/800/171/a/r3/final
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-nist-800-171a-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	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.01.01.ODP[01]	Account Management	the time period for account inactivity before disabling is defined.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
A.03.01.01.ODP[01]	Account Management	the time period for account inactivity before disabling is defined.	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	
A.03.01.01.ODP[02]	Account Management	the time period within which to notify account managers and designated personnel or roles when accounts are no longer required is defined.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
A.03.01.01.ODP[03]	Account Management	the time period within which to notify account managers and designated personnel or roles when users are terminated or transferred is defined.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
A.03.01.01.ODP[04]	Account Management	the time period within which to notify account managers and designated personnel or roles when system usage or the need-to-know changes for an individual is defined.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
A.03.01.01.ODP[05]	Account Management	the time period of expected inactivity requiring users to log out of the system is defined.	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.	5	
A.03.01.01.ODP[06]	Account Management	circumstances requiring users to log out of the system are defined.	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.	5	
A.03.01.01.a[01]	Account Management	system account types allowed are defined.	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	
A.03.01.01.a[01]	Account Management	system account types allowed are defined.	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	
A.03.01.01.a[02]	Account Management	system account types prohibited are defined.	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	
A.03.01.01.a[02]	Account Management	system account types prohibited are defined.	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	
A.03.01.01.b[01]	Account Management	system accounts are created in accordance with organizational policy, procedures, prerequisites, and criteria.	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	
A.03.01.01.b[01]	Account Management	system accounts are created in accordance with organizational policy, procedures, prerequisites, and criteria.	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	
A.03.01.01.b[02]	Account Management	system accounts are enabled in accordance with organizational policy, procedures, prerequisites, and criteria.	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	
A.03.01.01.b[02]	Account Management	system accounts are enabled in accordance with organizational policy, procedures, prerequisites, and criteria.	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	
A.03.01.01.b[03]	Account Management	system accounts are modified in accordance with organizational policy, procedures, prerequisites, and criteria.	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	
A.03.01.01.b[03]	Account Management	system accounts are modified in accordance with organizational policy, procedures, prerequisites, and criteria.	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	
A.03.01.01.b[04]	Account Management	system accounts are disabled in accordance with organizational policy, procedures, prerequisites, and criteria.	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	
A.03.01.01.b[04]	Account Management	system accounts are disabled in accordance with organizational policy, procedures, prerequisites, and criteria.	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	
A.03.01.01.b[05]	Account Management	system accounts are removed in accordance with organizational policy, procedures, prerequisites, and criteria.	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	
A.03.01.01.b[05]	Account Management	system accounts are removed in accordance with organizational policy, procedures, prerequisites, and criteria.	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	
A.03.01.01.c.01	Account Management	authorized users of the system are specified.	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	
A.03.01.01.c.01	Account Management	authorized users of the system are specified.	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	
A.03.01.01.c.02	Account Management	group and role memberships are specified.	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	
A.03.01.01.c.03	Account Management	access authorizations (i.e., privileges) for each account are specified.	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	
A.03.01.01.d.01	Account Management	access to the system is authorized based on a valid access authorization.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
A.03.01.01.d.02	Account Management	access to the system is authorized based on intended system usage.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
A.03.01.01.e	Account Management	the use of system accounts is monitored.	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	
A.03.01.01.f.01	Account Management	system accounts are disabled when 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	
A.03.01.01.f.02	Account Management	system accounts are disabled when the accounts have been inactive for <A.03.01.01.ODP[01]: time period>.	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	US DoD ODP Value: at most 90 days
A.03.01.01.f.02	Account Management	system accounts are disabled when the accounts have been inactive for <A.03.01.01.ODP[01]: 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	US DoD ODP Value: at most 90 days
A.03.01.01.f.03	Account Management	system accounts are disabled when 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	
A.03.01.01.f.04	Account Management	system accounts are disabled when the accounts violate organizational policy.	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	
A.03.01.01.f.05	Account Management	system accounts are disabled when 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	
A.03.01.01.g.01	Account Management	account managers and designated personnel or roles are notified within <A.03.01.01.ODP[02]: 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	US DoD ODP Value: 24 hours
A.03.01.01.g.02	Account Management	account managers and designated personnel or roles are notified within <A.03.01.01.ODP[03]: 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.	8	US DoD ODP Value: 24 hours
A.03.01.01.g.03	Account Management	account managers and designated personnel or roles are notified within <A.03.01.01.ODP[04]: 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.	8	US DoD ODP Value: 24 hours
A.03.01.01.h	Account Management	users are required to log out of the system after <A.03.01.01.ODP[05]: time period> of expected inactivity or when the following circumstances occur: <A.03.01.01.ODP[06]: circumstances>.	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.	8	US DoD ODP Values: [05] - at most 24 hours [06] - the work period ends, for privileged users at a minimum
03.01.02	Access Enforcement	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.01.02[01]	Access Enforcement	approved authorizations for logical access to CUI are enforced 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	
A.03.01.02[02]	Access Enforcement	approved authorizations for logical access to system resources are enforced in accordance with applicable access control policies.	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	
03.01.03	Information Flow Enforcement	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.01.03[01]	Information Flow Enforcement	approved authorizations are enforced for controlling the flow of CUI within 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	
A.03.01.03[01]	Information Flow Enforcement	approved authorizations are enforced for controlling the flow of CUI within the system.	Functional	Subset Of	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	10	
A.03.01.03[02]	Information Flow Enforcement	approved authorizations are enforced for controlling the flow of CUI 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	
A.03.01.03[02]	Information Flow Enforcement	approved authorizations are enforced for controlling the flow of CUI 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	
03.01.04	Separation of Duties	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.01.04.a	Separation of Duties	duties of individuals requiring separation are identified.	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	
03.01.05	Least Privilege	Determine If:	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
A.03.01.05.ODP[01]	Least Privilege	security functions for authorized access are defined.	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	
A.03.01.05.ODP[02]	Least Privilege	security-relevant information for authorized access is defined.	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	
A.03.01.05.ODP[03]	Least Privilege	the frequency at which to review the privileges assigned to roles or classes of users is defined.	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	
A.03.01.05.a	Least Privilege	system access for users (or processes acting on behalf of users) is authorized only when necessary to accomplish assigned organizational tasks.	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
A.03.01.05.b[01]	Least Privilege	access to <A.03.01.05.ODP[01]: security functions> is authorized.	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	US DoD ODP Value: 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
A.03.01.05.b[01]	Least Privilege	access to <A.03.01.05.ODP[01]: security functions> is authorized.	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	US DoD ODP Value: 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
A.03.01.05.b[02]	Least Privilege	access to <A.03.01.05.ODP[02]: security-relevant information> is authorized.	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	US DoD ODP Value: 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
A.03.01.05.b[02]	Least Privilege	access to <A.03.01.05.ODP[02]: security-relevant information> is authorized.	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	US DoD ODP Value: 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
A.03.01.05.c	Least Privilege	the privileges assigned to roles or classes of users are reviewed <A.03.01.05.ODP[03]: 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.	8	US DoD ODP Value: at least every 12 months
A.03.01.05.d	Least Privilege	privileges are reassigned or removed, 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	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.01.06.ODP[01]	Least Privilege – Privileged Accounts	personnel or roles to which privileged accounts on the system are to be restricted are defined.	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	
A.03.01.06.a	Least Privilege – Privileged Accounts	privileged accounts on the system are restricted to <A.03.01.06.ODP[01]: 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	US DoD ODP Value: only defined and authorized personnel or administrative roles
A.03.01.06.b	Least Privilege – Privileged Accounts	users (or roles) with privileged accounts are required to use non-privileged accounts when accessing non-security functions or non-security 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	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.01.07.a	Least Privilege – Privileged Functions	non-privileged users are prevented from executing privileged functions.	Functional	Intersects With	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.	5	
A.03.01.07.b	Least Privilege – Privileged Functions	the execution of privileged functions is logged.	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	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.01.08.ODP[01]	Unsuccessful Logon Attempts	the number of consecutive invalid logon attempts by a user allowed during a time period is defined.	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.	5	
A.03.01.08.ODP[02]	Unsuccessful Logon Attempts	the time period to which the number of consecutive invalid logon attempts by a user is limited is defined.	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.	5	
A.03.01.08.ODP[03]	Unsuccessful Logon Attempts	one or more of the following PARAMETER VALUES are selected: {the account or node is locked automatically for <A.03.01.08.ODP[04]: time period>; the account or node is locked automatically until released by an administrator; the next logon prompt is delayed automatically; the system administrator is notified automatically; other action is taken automatically}.	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	US DoD ODP Value: at least 15- minute time period
A.03.01.08.ODP[04]	Unsuccessful Logon Attempts	the time period for an account or node to be locked is defined (if selected).	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.	5	
A.03.01.08.a	Unsuccessful Logon Attempts	a limit of <A.03.01.08.ODP[01]: number> consecutive invalid logon attempts by a user during <A.03.01.08.ODP[02]: time period> is enforced.	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	US DoD ODP Values: [01] - at most five (5) [02] - period of five (5) minutes
A.03.01.08.b	Unsuccessful Logon Attempts	<A.03.01.08.ODP[03]: SELECTED PARAMETER VALUES> 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	US DoD 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	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.01.09	System Use Notification	a system use notification message with privacy and security notices consistent with applicable CUI rules is displayed before granting access to the system.	Functional	Intersects With	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).	5	
A.03.01.09	System Use Notification	a system use notification message with privacy and security notices consistent with applicable CUI rules is displayed 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.	5	
A.03.01.09	System Use Notification	a system use notification message with privacy and security notices consistent with applicable CUI rules is displayed 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.).	5	
03.01.10	Device Lock	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.01.10.ODP[01]	Device Lock	one or more of the following PARAMETER VALUES are selected: {a device lock is initiated after <A.03.01.10.ODP[02]: time period> of inactivity; the user is required to initiate a device lock before leaving the system unattended}.	Functional	Intersects With	Session Lock	IAC-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods.	8	US DoD ODP Value: at most 15- minute time period
A.03.01.10.ODP[02]	Device Lock	the time period of inactivity after which a device lock is initiated is defined (if selected).	Functional	Intersects With	Session Lock	IAC-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods.	5	
A.03.01.10.a	Device Lock	access to the system is prevented by <A.03.01.10.ODP[01]: SELECTED PARAMETER VALUES>.	Functional	Intersects With	Session Lock	IAC-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods.	8	US DoD 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
A.03.01.10.b	Device Lock	the device lock is retained until the user reestablishes access using established identification and authentication procedures.	Functional	Intersects With	Session Lock	IAC-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods.	5	
A.03.01.10.c	Device Lock	information previously visible on the display is concealed via device lock with a publicly viewable image.	Functional	Intersects With	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.	5	
03.01.11	Session Termination	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.01.11.ODP[01]	Session Termination	conditions or trigger events that require session disconnect are defined.	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.	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
A.03.01.11	Session Termination	a user session is terminated automatically after <A.03.01.11.ODP[01]: conditions or trigger events>.	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.	8	US DoD 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	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.01.12.a[01]	Remote Access	types of allowable remote system access are defined.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
A.03.01.12.a[02]	Remote Access	usage restrictions are established 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	
A.03.01.12.a[03]	Remote Access	configuration requirements are established 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	
A.03.01.12.a[04]	Remote Access	connection requirements are established 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	
A.03.01.12.b	Remote Access	each type of remote system access is authorized 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	
A.03.01.12.c[01]	Remote Access	remote access to the system is routed through authorized access control points.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
A.03.01.12.c[02]	Remote Access	remote access to the system is routed through 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	
A.03.01.12.d[1]	Remote Access	remote execution of privileged commands is authorized.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
A.03.01.12.d[1]	Remote Access	remote execution of privileged commands is authorized.	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	
A.03.01.12.d[2]	Remote Access	remote access to security-relevant information is authorized.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
A.03.01.12.d[2]	Remote Access	remote access to security-relevant information is authorized.	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	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.01.14	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.01.15	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.01.16	Wireless Access	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.01.16.a[01]	Wireless Access	each type of wireless access to the system is defined.	Functional	Intersects With	Guest Networks	NET-02.2	Mechanisms exist to implement and manage a secure guest network.	5	
A.03.01.16.a[01]	Wireless Access	each type of wireless access to the system is defined.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
A.03.01.16.a[02]	Wireless Access	usage restrictions are established 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	
A.03.01.16.a[02]	Wireless Access	usage restrictions are established 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	
A.03.01.16.a[03]	Wireless Access	configuration requirements are established 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	
A.03.01.16.a[04]	Wireless Access	connection requirements are established 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	
A.03.01.16.a[04]	Wireless Access	connection requirements are established 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	
A.03.01.16.b	Wireless Access	each type of wireless access to the system is authorized prior to establishing such connections.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
A.03.01.16.b	Wireless Access	each type of wireless access to the system is authorized prior to establishing such connections.	Functional	Intersects With	Guest Networks	NET-02.2	Mechanisms exist to implement and manage a secure guest network.	5	
A.03.01.16.c	Wireless Access	wireless networking capabilities not intended for use are disabled prior to issuance and deployment.	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	
A.03.01.16.d[01]	Wireless Access	wireless access to the system is protected using authentication.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
A.03.01.16.d[02]	Wireless Access	wireless access to the system is protected using encryption.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
03.01.17	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.01.18	Access Control for Mobile Devices	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.01.18.a[01]	Access Control for Mobile Devices	usage restrictions are established 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	
A.03.01.18.a[02]	Access Control for Mobile Devices	configuration requirements are established 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	
A.03.01.18.a[03]	Access Control for Mobile Devices	connection requirements are established for mobile devices.	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	
A.03.01.18.b	Access Control for Mobile Devices	the connection of mobile devices to the system is authorized.	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	
A.03.01.18.c	Access Control for Mobile Devices	full-device or container-based encryption is implemented 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	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.01.20	Use of External Systems	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.01.20.ODP[01]	Use of External Systems	security requirements to be satisfied on external systems prior to allowing the use of or access to those systems by authorized individuals are defined.	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	
A.03.01.20.a	Use of External Systems	the use of external systems is prohibited 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	
A.03.01.20.b	Use of External Systems	the following security requirements to be satisfied on external systems prior to allowing the use of or access to those systems by authorized individuals are established: <A.03.01.20.ODP[01]: 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	US DoD 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.
A.03.01.20.c.01	Use of External Systems	authorized individuals are permitted to use external systems to access the organizational system or to process, store, or transmit CUI only after verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied.	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	
A.03.01.20.c.02	Use of External Systems	authorized individuals are permitted to use external systems to access the organizational system or to process, store, or transmit CUI only after retaining approved system connection or processing agreements with the organizational entity 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	
A.03.01.20.d	Use of External Systems	the use of organization-controlled portable storage devices by authorized individuals on external systems is restricted.	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	
03.01.21	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.01.22	Publicly Accessible Content	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.01.22.a	Publicly Accessible Content	authorized individuals are trained 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	
A.03.01.22.b[01]	Publicly Accessible Content	the content on publicly accessible systems is reviewed for CUI.	Functional	Intersects With	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	5	
A.03.01.22.b[02]	Publicly Accessible Content	CUI is removed from publicly accessible systems, if discovered.	Functional	Intersects With	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	5	
A.03.01.22.b[02]	Publicly Accessible Content	CUI is removed from publicly accessible systems, if discovered.	Functional	Intersects With	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive/regulated data spills.	5	
03.02.01	Literacy Training and Awareness	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.02.01.ODP[01]	Literacy Training and Awareness	the frequency at which to provide security literacy training to system users after initial training is defined.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
A.03.02.01.ODP[02]	Literacy Training and Awareness	events that require security literacy training for system users are defined.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
A.03.02.01.ODP[03]	Literacy Training and Awareness	the frequency at which to update security literacy training content is defined.	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	
A.03.02.01.ODP[04]	Literacy Training and Awareness	events that require security literacy training content updates are defined.	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	
A.03.02.01.a.01[01]	Literacy Training and Awareness	security literacy training is provided to system users as part of initial training for new 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	
A.03.02.01.a.01[02]	Literacy Training and Awareness	security literacy training is provided to system users <A.03.02.01.ODP[01]: frequency> after initial training.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	US DoD ODP Value: at least every 12 months
A.03.02.01.a.02	Literacy Training and Awareness	security literacy training is provided to system users when required by system changes or following <A.03.02.01.ODP[02]: 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.	8	US DoD ODP Value: significant, novel incidents, or significant changes to risks
A.03.02.01.a.03[01]	Literacy Training and Awareness	security literacy training is provided to system users on recognizing indicators of insider threat.	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	
A.03.02.01.a.03[02]	Literacy Training and Awareness	security literacy training is provided to system users on reporting indicators of insider threat.	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	
A.03.02.01.a.03[03]	Literacy Training and Awareness	security literacy training is provided to system users on recognizing indicators of social engineering.	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	
A.03.02.01.a.03[04]	Literacy Training and Awareness	security literacy training is provided to system users on reporting indicators of social engineering.	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	
A.03.02.01.a.03[05]	Literacy Training and Awareness	security literacy training is provided to system users on recognizing indicators of 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	
A.03.02.01.a.03[06]	Literacy Training and Awareness	security literacy training is provided to system users on reporting indicators of 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	
A.03.02.01.b[01]	Literacy Training and Awareness	security literacy training content is updated <A.03.02.01.ODP[03]: frequency>.	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.	8	US DoD ODP Value: at least every 12 months
A.03.02.01.b[02]	Literacy Training and Awareness	security literacy training content is updated following <A.03.02.01.ODP[04]: 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.	8	US DoD ODP Value: significant, novel incidents, or significant changes to risks
03.02.02	Role-Based Training	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.02.02.ODP[01]	Role-Based Training	the frequency at which to provide role-based security training to assigned personnel after initial training is defined.	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	
A.03.02.02.ODP[02]	Role-Based Training	events that require role-based security training are defined.	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	
A.03.02.02.ODP[03]	Role-Based Training	the frequency at which to update role-based security training content is defined.	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	
A.03.02.02.ODP[04]	Role-Based Training	events that require role-based security training content updates are defined.	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	
A.03.02.02.a.01[01]	Role-Based Training	role-based security training is provided to organizational personnel before authorizing access to the system or 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	
A.03.02.02.a.01[02]	Role-Based Training	role-based security training is provided to organizational personnel before performing assigned duties.	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	
A.03.02.02.a.01[03]	Role-Based Training	role-based security training is provided to organizational personnel <A.03.02.02.ODP[01]: frequency> after initial training.	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	US DoD ODP Value: at least every 12 months
A.03.02.02.a.02	Role-Based Training	role-based security training is provided to organizational personnel when required by system changes or following <A.03.02.02.ODP[02]: events>.	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	US DoD ODP Value: significant, novel incidents, or significant changes to risks
A.03.02.02.b[01]	Role-Based Training	role-based security training content is updated <A.03.02.02.ODP[03]: frequency>.	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	US DoD ODP Value: at least every 12 months
A.03.02.02.b[02]	Role-Based Training	role-based security training content is updated following <A.03.02.02.ODP[04]: events>.	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	US DoD ODP Value: significant, novel incidents, or significant changes to risks
03.02.03	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.03.01	Event Logging	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.03.01.ODP[01]	Event Logging	event types selected for logging within the system are defined.	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: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
A.03.03.01.ODP[02]	Event Logging	the frequency of event types selected for logging are reviewed and updated.	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
A.03.03.01.a	Event Logging	the following event types are specified for logging within the system: <A.03.03.01.ODP[01]: 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: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	8	applicable: (1) Authentication events: (a) Logons (Success/Failure) (b) Logoffs (Success) (2) Security Relevant File and Objects events: (a) Create (Success/Failure) (b) Access (Success/Failure) (c) Delete (Success/Failure) (d) Modify (Success/Failure) (e) Permission Modification (Success/Failure) (f) Ownership Modification (Success/Failure) (3) Export/Writes/downloads to devices/digital media (e.g., CD/DVD, USB, SD) (Success/Failure) (4) Import/Uploads from devices/digital media (e.g., CD/DVD, USB, SD) (Success/Failure) (5) User and Group Management events: (a) User add, delete, modify, disable, lock (Success/Failure) (b) Group/Role add, delete, modify (Success/Failure) (6) Use of Privileged/Special Rights events: (a) Security or audit policy changes (Success/Failure) (b) Configuration changes (Success/Failure) (7) Admin or root-level access (Success/Failure) (8) Privilege/Role escalation (Success/Failure) (9) Audit and security relevant log data accesses (Success/Failure) (10) System reboot, restart, and shutdown (Success/Failure) (11) Print to a device (Success/Failure) (12) Print to a file (e.g., pdf format) (Success/Failure) (13) Application (e.g., Adobe, Firefox, MS Office
A.03.03.01.b[01]	Event Logging	the event types selected for logging are reviewed <A.03.03.01.ODP[02]: frequency>.	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	8	US DoD ODP Value: at least every 12 months and after any significant incidents or significant changes to risks

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
A.03.03.01.b[02]	Event Logging	the event types selected for logging are updated <A.03.03.01.ODP[02]: frequency>.	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: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	8	US DoD ODP Value: at least every 12 months and after any significant incidents or significant changes to risks
03.03.02	Audit Record Content	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.03.02.a.01	Audit Record Content	audit records contain information that establishes what type of event occurred.	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.	5	
A.03.03.02.a.02	Audit Record Content	audit records contain information that establishes 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: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
A.03.03.02.a.03	Audit Record Content	audit records contain information that establishes 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: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
A.03.03.02.a.04	Audit Record Content	audit records contain information that establishes the 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: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
A.03.03.02.a.05	Audit Record Content	audit records contain information that establishes the 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: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
A.03.03.02.a.06	Audit Record Content	audit records contain information that establishes the 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: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
A.03.03.02.b	Audit Record Content	additional information for audit records is provided, 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: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
A.03.03.02.b	Audit Record Content	additional information for audit records is provided, 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: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	5	
03.03.03	Audit Record Generation	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.03.03.a	Audit Record Generation	audit records for the selected event types and audit record content specified in 03.03.01 and 03.03.02 are generated.	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.	5	
A.03.03.03.b	Audit Record Generation	audit records are retained 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	
A.03.03.03.b	Audit Record Generation	audit records are retained for a time period consistent with the records retention policy.	Functional	Intersects With	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.	5	
03.03.04	Response to Audit Logging Process Failures	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.03.04.ODP[01]	Response to Audit Logging Process Failures	the time period for organizational personnel or roles receiving audit logging process failure alerts is defined.	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.	5	
A.03.03.04.ODP[02]	Response to Audit Logging Process Failures	additional actions to be taken in the event of an audit logging process failure are defined.	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.	5	
A.03.03.04.a	Response to Audit Logging Process Failures	organizational personnel or roles are alerted in the event of an audit logging process failure within <A.03.03.04.ODP[01]: time period>.	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	US DoD ODP Value: near real time or as soon as practicable upon discovery
A.03.03.04.b	Response to Audit Logging Process Failures	the following additional actions are taken: <A.03.03.04.ODP[02]: 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	US DoD 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	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.03.05.ODP[01]	Audit Record Review, Analysis, and Reporting	the frequency at which system audit records are reviewed and analyzed is defined.	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
A.03.03.05.ODP[01]	Audit Record Review, Analysis, and Reporting	the frequency at which system audit records are reviewed and analyzed is defined.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
A.03.03.05.a	Audit Record Review, Analysis, and Reporting	system audit records are reviewed and analyzed <A.03.03.05.ODP[01]: frequency> for indications and the potential impact of inappropriate or unusual activity.	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	8	US DoD ODP Value: at least weekly
A.03.03.05.a	Audit Record Review, Analysis, and Reporting	system audit records are reviewed and analyzed <A.03.03.05.ODP[01]: 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.	8	US DoD ODP Value: at least weekly
A.03.03.05.b	Audit Record Review, Analysis, and Reporting	findings are reported 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.	5	
A.03.03.05.b	Audit Record Review, Analysis, and Reporting	findings are reported 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.	5	
A.03.03.05.c[01]	Audit Record Review, Analysis, and Reporting	audit records across different repositories are analyzed 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.	5	
A.03.03.05.c[02]	Audit Record Review, Analysis, and Reporting	audit records across different repositories are correlated to gain organization-wide situational awareness.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
03.03.06	Audit Record Reduction and Report Generation	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.03.06.a[01]	Audit Record Reduction and Report Generation	an audit record reduction and report generation capability that supports audit record review is implemented.	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	
A.03.03.06.a[02]	Audit Record Reduction and Report Generation	an audit record reduction and report generation capability that supports audit record analysis is implemented.	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	
A.03.03.06.a[03]	Audit Record Reduction and Report Generation	an audit record reduction and report generation capability that supports audit record reporting requirements is implemented.	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	
A.03.03.06.a[04]	Audit Record Reduction and Report Generation	an audit record reduction and report generation capability that supports after-the-fact investigations of incidents is implemented.	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	

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
A.03.03.06.b[01]	Audit Record Reduction and Report Generation	the original content of audit records is preserved.	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	
A.03.03.06.b[02]	Audit Record Reduction and Report Generation	the original time ordering of audit records is preserved.	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	
03.03.07	Time Stamps	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.03.07.ODP[01]	Time Stamps	granularity of time measurement for audit record time stamps is defined.	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	
A.03.03.07.a	Time Stamps	internal system clocks are used to generate time stamps for audit records.	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	
A.03.03.07.b[01]	Time Stamps	time stamps are recorded for audit records that meet <A.03.03.07.ODP[01]: granularity of time measurement>.	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.	8	US DoD ODP Value: a granularity of one (1) second or smaller
A.03.03.07.b[02]	Time Stamps	time stamps are recorded for audit records 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	Intersects With	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	5	
03.03.08	Protection of Audit Information	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.03.08.a[01]	Protection of Audit Information	audit information is protected 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	
A.03.03.08.a[02]	Protection of Audit Information	audit logging tools are protected from unauthorized access, modification, and deletion.	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	
A.03.03.08.b	Protection of Audit Information	access to management of audit logging functionality is authorized to only a subset of privileged users or roles.	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	
A.03.03.08.b	Protection of Audit Information	access to management of audit logging functionality is authorized to only a subset of privileged users or roles.	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	
03.03.09	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.04.01	Baseline Configuration	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.04.01.ODP[01]	Baseline Configuration	the frequency of baseline configuration review and update is defined.	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	5	
A.03.04.01.a[01]	Baseline Configuration	a current baseline configuration of the system is developed.	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	
A.03.04.01.a[02]	Baseline Configuration	a current baseline configuration of the system is maintained under configuration control.	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	
A.03.04.01.b[01]	Baseline Configuration	the baseline configuration of the system is reviewed <A.03.04.01.ODP[01]: frequency>.	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	8	US DoD ODP Value: at least every 12 months and after any significant incidents or significant changes occur
A.03.04.01.b[02]	Baseline Configuration	the baseline configuration of the system is updated <A.03.04.01.ODP[01]: frequency>.	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	8	US DoD ODP Value: at least every 12 months and after any significant incidents or significant changes occur
A.03.04.01.b[03]	Baseline Configuration	the baseline configuration of the system is reviewed when system components are installed or modified.	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	5	
A.03.04.01.b[04]	Baseline Configuration	the baseline configuration of the system is updated when system components are installed or modified.	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	5	
03.04.02	Configuration Settings	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.04.02.ODP[01]	Configuration Settings	configuration settings for the system that reflect the most restrictive mode consistent with operational requirements are defined.	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	
A.03.04.02.a[01]	Configuration Settings	the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements are established and documented: <A.03.04.02.ODP[01]: 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	US DoD 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 (https://ncp.nist.gov/repository) 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.
A.03.04.02.a[02]	Configuration Settings	the following configuration settings for the system are implemented: <A.03.04.02.ODP[01]: 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	US DoD 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 (https://ncp.nist.gov/repository) 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.
A.03.04.02.b[01]	Configuration Settings	any deviations from established configuration settings are identified and documented.	Functional	Intersects With	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	5	
A.03.04.02.b[02]	Configuration Settings	any deviations from established configuration settings are approved.	Functional	Intersects With	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	5	
03.04.03	Configuration Change Control	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.04.03.a	Configuration Change Control	the types of changes to the system that are configuration-controlled are defined.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
A.03.04.03.a	Configuration Change Control	the types of changes to the system that are configuration-controlled are defined.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
A.03.04.03.b[01]	Configuration Change Control	proposed configuration-controlled changes to the system are reviewed 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	
A.03.04.03.b[02]	Configuration Change Control	proposed configuration-controlled changes to the system are approved or disapproved with explicit consideration for security impacts.	Functional	Intersects With	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	5	
A.03.04.03.c[01]	Configuration Change Control	approved configuration-controlled changes to the system are implemented.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
A.03.04.03.c[01]	Configuration Change Control	approved configuration-controlled changes to the system are implemented.	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).	5	
A.03.04.03.c[02]	Configuration Change Control	approved configuration-controlled changes to the system are documented.	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	
A.03.04.03.d[01]	Configuration Change Control	activities associated with configuration-controlled changes to the system are monitored.	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	
A.03.04.03.d[01]	Configuration Change Control	activities associated with configuration-controlled changes to the system are monitored.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
A.03.04.03.d[02]	Configuration Change Control	activities associated with configuration-controlled changes to the system are reviewed.	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	
A.03.04.03.d[02]	Configuration Change Control	activities associated with configuration-controlled changes to the system are reviewed.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
03.04.04	Impact Analyses	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.04.04.a	Impact Analyses	changes to the system are analyzed 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.	5	
A.03.04.04.b	Impact Analyses	the security requirements for the system continue to be satisfied after the system changes have been implemented.	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	5	

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
03.04.05	Access Restrictions for Change	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.04.05[01]	Access Restrictions for Change	physical access restrictions associated with changes to the system are defined and documented.	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	
A.03.04.05[02]	Access Restrictions for Change	physical access restrictions associated with changes to the system are approved.	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	
A.03.04.05[03]	Access Restrictions for Change	physical access restrictions associated with changes to the system are enforced.	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	
A.03.04.05[04]	Access Restrictions for Change	logical access restrictions associated with changes to the system are defined and documented.	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	
A.03.04.05[05]	Access Restrictions for Change	logical access restrictions associated with changes to the system are approved.	Functional	Intersects With	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	5	
A.03.04.05[06]	Access Restrictions for Change	logical access restrictions associated with changes to the system are enforced.	Functional	Intersects With	Permissions To Implement Changes	CHG-04.4	Mechanisms exist to limit operational privileges for implementing changes.	5	
03.04.06	Least Functionality	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.04.06.ODP[01]	Least Functionality	functions to be prohibited or restricted are defined.	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	
A.03.04.06.ODP[02]	Least Functionality	ports to be prohibited or restricted are defined.	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	
A.03.04.06.ODP[03]	Least Functionality	protocols to be prohibited or restricted are defined.	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	
A.03.04.06.ODP[04]	Least Functionality	connections to be prohibited or restricted are defined.	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	
A.03.04.06.ODP[05]	Least Functionality	services to be prohibited or restricted are defined.	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	
A.03.04.06.ODP[06]	Least Functionality	the frequency at which to review the system to identify unnecessary or nonsecure functions, ports, protocols, connections, or services is defined.	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.	5	
A.03.04.06.b[01]	Least Functionality	the use of the following functions is prohibited or restricted: <A.03.04.06.ODP[01]: functions>.	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	US DoD 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.
A.03.04.06.b[02]	Least Functionality	the use of the following ports is prohibited or restricted: <A.03.04.06.ODP[02]: ports>.	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	US DoD 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.
A.03.04.06.b[03]	Least Functionality	the use of the following protocols is prohibited or restricted: <A.03.04.06.ODP[03]: protocols>.	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	US DoD 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.
A.03.04.06.b[04]	Least Functionality	the use of the following connections is prohibited or restricted: <A.03.04.06.ODP[04]: connections>.	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	US DoD 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.
A.03.04.06.b[05]	Least Functionality	the use of the following services is prohibited or restricted: <A.03.04.06.ODP[05]: services>.	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	US DoD 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.
A.03.04.06.c	Least Functionality	the system is reviewed <A.03.04.06.ODP[06]: frequency> to identify unnecessary or nonsecure functions, ports, protocols, connections, and services.	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	8	US DoD ODP Value: at least every 12 months, when any system functions, ports, protocols, or services changes are made, and after any significant incidents or significant changes to risks

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
A.03.04.06.d	Least Functionality	unnecessary or nonsecure functions, ports, protocols, connections, and services are disabled or removed.	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	
03.04.07	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.04.08	Authorized Software – Allow by Exception	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.04.08.ODP[01]	Authorized Software – Allow by Exception	the frequency at which to review and update the list of authorized software programs is defined.	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	
A.03.04.08.a	Authorized Software – Allow by Exception	software programs authorized to execute on the system are identified.	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	
A.03.04.08.b	Authorized Software – Allow by Exception	a deny-all, allow-by-exception policy for the execution of authorized software programs on the system is implemented.	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	
A.03.04.08.c	Authorized Software – Allow by Exception	the list of authorized software programs is reviewed and updated <A.03.04.08.ODP[01]: frequency>.	Functional	Intersects With	Approved Technologies	AST-01.4	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	8	US DoD ODP Value: at least quarterly
03.04.09	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.04.10	System Component Inventory	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.04.10.ODP[01]	System Component Inventory	the frequency at which to review and update the system component inventory is defined.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
A.03.04.10.a	System Component Inventory	an inventory of system components is developed and documented.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
A.03.04.10.b[01]	System Component Inventory	the system component inventory is reviewed <A.03.04.10.ODP[01]: frequency>.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	8	US DoD ODP Value: at least quarterly
A.03.04.10.b[02]	System Component Inventory	the system component inventory is updated <A.03.04.10.ODP[01]: frequency>.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	8	US DoD ODP Value: at least quarterly
A.03.04.10.c[01]	System Component Inventory	the system component inventory is updated as part of component installations.	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.	5	
A.03.04.10.c[02]	System Component Inventory	the system component inventory is updated as part of component removals.	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.	5	
A.03.04.10.c[03]	System Component Inventory	the system component inventory is updated as part of system updates.	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.	5	
03.04.11	Information Location	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.04.11.a[01]	Information Location	the location of CUI is identified and documented.	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/regulated data is stored, transmitted or processed.	5	
A.03.04.11.a[01]	Information Location	the location of CUI is identified and documented.	Functional	Intersects With	Information Location	DCH-24	Mechanisms exist to identify and document the location of information and the specific system components on which the information resides.	5	
A.03.04.11.a[02]	Information Location	the system components on which CUI is processed are identified and documented.	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/regulated data is stored, transmitted or processed.	5	
A.03.04.11.a[02]	Information Location	the system components on which CUI is processed are identified and documented.	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: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system	10	
A.03.04.11.a[03]	Information Location	the system components on which CUI is stored are identified and documented.	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/regulated data is stored, transmitted or processed.	5	
A.03.04.11.a[03]	Information Location	the system components on which CUI is stored are identified and documented.	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: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system	10	
A.03.04.11.b[01]	Information Location	changes to the system or system component location where CUI is processed are documented.	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/regulated data is stored, transmitted or processed.	5	
A.03.04.11.b[01]	Information Location	changes to the system or system component location where CUI is processed are documented.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5	
A.03.04.11.b[01]	Information Location	changes to the system or system component location where CUI is processed are documented.	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: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system	10	
A.03.04.11.b[02]	Information Location	changes to the system or system component location where CUI is stored are documented.	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/regulated data is stored, transmitted or processed.	5	
A.03.04.11.b[02]	Information Location	changes to the system or system component location where CUI is stored are documented.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5	
A.03.04.11.b[02]	Information Location	changes to the system or system component location where CUI is stored are documented.	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: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system	10	
03.04.12	System and Component Configuration for High-Risk Areas	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.04.12.ODP[01]	System and Component Configuration for High-Risk Areas	configurations for systems or system components to be issued to individuals traveling to high-risk locations are defined.	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	
A.03.04.12.ODP[02]	System and Component Configuration for High-Risk Areas	security requirements to be applied to the system or system components when individuals return from travel are defined.	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	
A.03.04.12.a	System and Component Configuration for High-Risk Areas	systems or system components with the following configurations are issued to individuals traveling to high-risk locations: <A.03.04.12.ODP[01]: configurations>.	Functional	Intersects With	Travel-Only Devices	AST-24	Mechanisms exist to issue personnel travelling overseas with temporary, loaner or "travel-only" end user technology (e.g., laptops and mobile devices) when travelling to authoritarian countries with a higher-than average risk for Intellectual Property (IP) theft or espionage against individuals and private companies.	8	US DoD 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
A.03.04.12.b	System and Component Configuration for High-Risk Areas	the following security requirements are applied to the system or system components when the individuals return from travel: <A.03.04.12.ODP[02]: 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	US DoD 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
03.05.01	User Identification and Authentication	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.05.01.ODP[01]	User Identification and Authentication	circumstances or situations that require re-authentication are defined.	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.	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
A.03.05.01.a[01]	User Identification and Authentication	system users are uniquely identified.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
A.03.05.01.a[02]	User Identification and Authentication	system users are authenticated.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
A.03.05.01.a[03]	User Identification and Authentication	processes acting on behalf of users are associated with uniquely identified and authenticated system 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.	5	
A.03.05.01.b	User Identification and Authentication	users are reauthenticated when <A.03.05.01.ODP[01]: circumstances or situations>.	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	US DoD 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	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.05.02.ODP[01]	Device Identification and Authentication	devices or types of devices to be uniquely identified and authenticated before establishing a connection are defined.	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	
A.03.05.02[01]	Device Identification and Authentication	<A.03.05.02.ODP[01]: devices or types of devices> are uniquely identified 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	US DoD ODP Value: all devices for identification, where feasible for authentication, and document when not feasible
A.03.05.02[02]	Device Identification and Authentication	<A.03.05.02.ODP[01]: devices or types of devices> are authenticated 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	US DoD ODP Value: all devices for identification, where feasible for authentication, and document when not feasible
03.05.03	Multi-Factor Authentication	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.05.03[01]	Multi-Factor Authentication	multi-factor authentication for access to privileged accounts is implemented.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	5	
A.03.05.03[01]	Multi-Factor Authentication	multi-factor authentication for access to privileged accounts is implemented.	Functional	Intersects With	Out-of-Band Multi-Factor Authentication	IAC-06.4	Mechanisms exist to implement Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.	5	
A.03.05.03[02]	Multi-Factor Authentication	multi-factor authentication for access to non-privileged accounts is implemented.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	5	
A.03.05.03[02]	Multi-Factor Authentication	multi-factor authentication for access to non-privileged accounts is implemented.	Functional	Intersects With	Out-of-Band Multi-Factor Authentication	IAC-06.4	Mechanisms exist to implement Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.	5	
03.05.04	Replay-Resistant Authentication	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.05.04[01]	Replay-Resistant Authentication	replay-resistant authentication mechanisms for access to privileged accounts are implemented.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baselines configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
A.03.05.04[01]	Replay-Resistant Authentication	replay-resistant authentication mechanisms for access to privileged accounts are implemented.	Functional	Intersects With	Replay-Resistant Authentication	IAC-02.2	Automated mechanisms exist to employ replay-resistant authentication.	5	
A.03.05.04[02]	Replay-Resistant Authentication	replay-resistant authentication mechanisms for access to non-privileged accounts are implemented.	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	
A.03.05.04[02]	Replay-Resistant Authentication	replay-resistant authentication mechanisms for access to non-privileged accounts are implemented.	Functional	Intersects With	Replay-Resistant Authentication	IAC-02.2	Automated mechanisms exist to employ replay-resistant authentication.	5	
03.05.05	Identifier Management	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.05.05.ODP[01]	Identifier Management	the time period for preventing the reuse of identifiers is defined.	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	
A.03.05.05.ODP[02]	Identifier Management	characteristic used to identify individual status are defined.	Functional	Intersects With	Identity User Status	IAC-09.2	Mechanisms exist to identify contractors and other third-party users through unique username characteristics.	5	
A.03.05.05.a	Identifier Management	authorization is received 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.	5	
A.03.05.05.b[01]	Identifier Management	an identifier that identifies an individual, group, role, service, or device is selected.	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	
A.03.05.05.b[02]	Identifier Management	an identifier that identifies an individual, group, role, service, or device is assigned.	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	
A.03.05.05.c	Identifier Management	the reuse of identifiers for <A.03.05.05.ODP[01]: time period> is prevented.	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	US DoD ODP Value: at least ten (10) years
A.03.05.05.d	Identifier Management	individual identifiers are managed by uniquely identifying each individual as <A.03.05.05.ODP[02]: characteristic>.	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	US DoD ODP Value: privileged or non-privileged users; contractors, foreign nationals, and/or non-organizational users
A.03.05.05.d	Identifier Management	individual identifiers are managed by uniquely identifying each individual as <A.03.05.05.ODP[02]: characteristic>.	Functional	Intersects With	Identity User Status	IAC-09.2	Mechanisms exist to identify contractors and other third-party users through unique username characteristics.	8	US DoD ODP Value: privileged or non-privileged users; contractors, foreign nationals, and/or non-organizational users
03.05.06	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.05.07	Password Management	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.05.07.ODP[01]	Password Management	the frequency at which to update the list of commonly used, expected, or compromised passwords is defined.	Functional	Intersects With	Automated Support For Password Strength	IAC-10.4	Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.	5	
A.03.05.07.ODP[01]	Password Management	the frequency at which to update the list of commonly used, expected, or compromised passwords is defined.	Functional	Intersects With	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	5	
A.03.05.07.ODP[02]	Password Management	password composition and complexity rules are defined.	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	
A.03.05.07.a[01]	Password Management	a list of commonly used, expected, or compromised passwords is maintained.	Functional	Intersects With	Automated Support For Password Strength	IAC-10.4	Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.	5	
A.03.05.07.a[01]	Password Management	a list of commonly used, expected, or compromised passwords is maintained.	Functional	Intersects With	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	5	
A.03.05.07.a[02]	Password Management	a list of commonly used, expected, or compromised passwords is updated <A.03.05.07.ODP[01]: frequency>.	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	US DoD ODP Value: at least quarterly
A.03.05.07.a[02]	Password Management	a list of commonly used, expected, or compromised passwords is updated <A.03.05.07.ODP[01]: frequency>.	Functional	Intersects With	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	8	US DoD ODP Value: at least quarterly
A.03.05.07.a[03]	Password Management	a list of commonly used, expected, or compromised passwords is updated 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.	5	
A.03.05.07.a[03]	Password Management	a list of commonly used, expected, or compromised passwords is updated 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.	5	
A.03.05.07.b	Password Management	passwords are verified not to be found on the list of commonly used, expected, or compromised passwords when they are created or updated by users.	Functional	Intersects With	Automated Support For Password Strength	IAC-10.4	Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.	5	
A.03.05.07.b	Password Management	passwords are verified not to be found on the list of commonly used, expected, or compromised passwords when they are created or updated by users.	Functional	Intersects With	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	5	
A.03.05.07.c	Password Management	passwords are only transmitted over cryptographically protected channels.	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	
A.03.05.07.c	Password Management	passwords are only transmitted over cryptographically protected channels.	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
A.03.05.07.d	Password Management	passwords are stored 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	
A.03.05.07.d	Password Management	passwords are stored 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.	5	
A.03.05.07.e	Password Management	a new password is selected 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.	5	
A.03.05.07.e	Password Management	a new password is selected upon first use after account recovery.	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
A.03.05.07.f	Password Management	the following composition and complexity rules for passwords are enforced: <A.03.05.07.ODP[02]: rules>.	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	US DoD ODP Values: (1) Must have a minimum length of 16 characters. (2) Contains a string of characters that does not include the user's account name or full name.
A.03.05.07.f	Password Management	the following composition and complexity rules for passwords are enforced: <A.03.05.07.ODP[02]: 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	US DoD ODP Values: (1) Must have a minimum length of 16 characters. (2) Contains a string of characters that does not include the user's account name or full name.
03.05.08	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.05.09	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.05.10	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.05.11	Authentication Feedback	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.05.11	Authentication Feedback	feedback of authentication information during the authentication process is obscured.	Functional	Intersects With	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.	5	
03.05.12	Authenticator Management	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.05.12.ODP[01]	Authenticator Management	the frequency for changing or refreshing authenticators is defined.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
A.03.05.12.ODP[02]	Authenticator Management	events that trigger the change or refreshment of authenticators are defined.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
A.03.05.12.a	Authenticator Management	the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution is verified.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
A.03.05.12.b	Authenticator Management	initial authenticator content for any authenticators issued by the organization is established.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
A.03.05.12.c[01]	Authenticator Management	administrative procedures for initial authenticator distribution are established.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
A.03.05.12.c[02]	Authenticator Management	administrative procedures for lost, compromised, or damaged authenticators are established.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
A.03.05.12.c[03]	Authenticator Management	administrative procedures for revoking authenticators are established.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
A.03.05.12.c[04]	Authenticator Management	administrative procedures for initial authenticator distribution are implemented.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
A.03.05.12.c[05]	Authenticator Management	administrative procedures for lost, compromised, or damaged authenticators are implemented.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
A.03.05.12.c[06]	Authenticator Management	administrative procedures for revoking authenticators are implemented.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
A.03.05.12.d	Authenticator Management	default authenticators are changed at first use.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
A.03.05.12.e	Authenticator Management	authenticators are changed or refreshed <A.03.05.12.ODP[01]: frequency> or when the following events occur: <A.03.05.12.ODP[02]: events>.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	8	US DoD ODP Values: (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. (2) after a relevant security incident or any evidence of compromise or loss.
A.03.05.12.f[01]	Authenticator Management	authenticator content is protected from unauthorized disclosure.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
A.03.05.12.f[01]	Authenticator Management	authenticator content is protected from unauthorized disclosure.	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
A.03.05.12.f[02]	Authenticator Management	authenticator content is protected from unauthorized modification.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
A.03.05.12.f[02]	Authenticator Management	authenticator content is protected from unauthorized modification.	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
03.06.01	Incident Handling	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.06.01[01]	Incident Handling	an incident-handling capability that is consistent with the incident response plan is implemented.	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	
A.03.06.01[02]	Incident Handling	the incident handling capability includes preparation.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
A.03.06.01[03]	Incident Handling	the incident handling capability includes detection and analysis.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
A.03.06.01[04]	Incident Handling	the incident handling capability includes containment.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
A.03.06.01[05]	Incident Handling	the incident handling capability includes eradication.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
A.03.06.01[06]	Incident Handling	the incident handling capability includes recovery.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
03.06.02	Incident Monitoring, Reporting, and Response Assistance	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.06.02.ODP[01]	Incident Monitoring, Reporting, and Response Assistance	the time period to report suspected incidents to the organizational incident response capability is defined.	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.	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
A.03.06.02.ODP[01]	Incident Monitoring, Reporting, and Response Assistance	the time period to report suspected incidents to the organizational incident response capability is defined.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
A.03.06.02.ODP[02]	Incident Monitoring, Reporting, and Response Assistance	authorities to whom incident information is to be reported are defined.	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.	5	
A.03.06.02.ODP[02]	Incident Monitoring, Reporting, and Response Assistance	authorities to whom incident information is to be reported are defined.	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	
A.03.06.02.ODP[02]	Incident Monitoring, Reporting, and Response Assistance	authorities to whom incident information is to be reported are defined.	Functional	Intersects With	Regulatory & Law Enforcement Contacts	IRO-14	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.	5	
A.03.06.02.a[01]	Incident Monitoring, Reporting, and Response Assistance	system security incidents are tracked.	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	
A.03.06.02.a[02]	Incident Monitoring, Reporting, and Response Assistance	system security incidents are documented.	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	
A.03.06.02.b	Incident Monitoring, Reporting, and Response Assistance	suspected incidents are reported to the organizational incident response capability within <A.03.06.02.ODP[01]: time period>.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	8	US DoD ODP Value: near real time or as soon as practicable upon discovery
A.03.06.02.b	Incident Monitoring, Reporting, and Response Assistance	suspected incidents are reported to the organizational incident response capability within <A.03.06.02.ODP[01]: time period>.	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	8	US DoD ODP Value: near real time or as soon as practicable upon discovery
A.03.06.02.b	Incident Monitoring, Reporting, and Response Assistance	suspected incidents are reported to the organizational incident response capability within <A.03.06.02.ODP[01]: time period>.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	8	US DoD ODP Value: near real time or as soon as practicable upon discovery
A.03.06.02.c	Incident Monitoring, Reporting, and Response Assistance	incident information is reported to <A.03.06.02.ODP[02]: authorities>.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	8	US DoD ODP Value: all applicable personnel and entities as specified by the contract, and in accordance with any incident response plan notification procedures
A.03.06.02.d	Incident Monitoring, Reporting, and Response Assistance	an incident response support resource that offers advice and assistance to system users on handling and reporting incidents is provided.	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	5	
A.03.06.02.d	Incident Monitoring, Reporting, and Response Assistance	an incident response support resource that offers advice and assistance to system users on handling and reporting incidents is provided.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
A.03.06.02.d	Incident Monitoring, Reporting, and Response Assistance	an incident response support resource that offers advice and assistance to system users on handling and reporting incidents is provided.	Functional	Intersects With	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.	5	
03.06.03	Incident Response Testing	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.06.03.ODP[01]	Incident Response Testing	the frequency at which to test the effectiveness of the incident response capability for the system is defined.	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5	
A.03.06.03	Incident Response Testing	the effectiveness of the incident response capability is tested <A.03.06.03.ODP[01]: frequency>.	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	8	US DoD ODP Value: at least every 12 months
03.06.04	Incident Response Training	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.06.04.ODP[01]	Incident Response Training	the time period within which incident response training is to be provided to system users is defined.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5	
A.03.06.04.ODP[02]	Incident Response Training	the frequency at which to provide incident response training to users after initial training is defined.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5	
A.03.06.04.ODP[03]	Incident Response Training	the frequency at which to review and update incident response training content is defined.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5	
A.03.06.04.ODP[04]	Incident Response Training	events that initiate a review of the incident response training content are defined.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5	
A.03.06.04.ODP[04]	Incident Response Training	events that initiate a review of the incident response training content are defined.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5	
A.03.06.04.a.01	Incident Response Training	incident response training for system users consistent with assigned roles and responsibilities is provided within <A.03.06.04.ODP[01]: time period> of assuming an incident response role or responsibility or acquiring system access.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	8	US DoD ODP Value: ten (10) days for privileged users, thirty (30) days for all other roles
A.03.06.04.a.01	Incident Response Training	incident response training for system users consistent with assigned roles and responsibilities is provided within <A.03.06.04.ODP[01]: 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: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	8	US DoD ODP Value: ten (10) days for privileged users, thirty (30) days for all other roles
A.03.06.04.a.02	Incident Response Training	incident response training for system users consistent with assigned roles and responsibilities is provided when required by system changes.	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	
A.03.06.04.a.03	Incident Response Training	incident response training for system users consistent with assigned roles and responsibilities is provided <A.03.06.04.ODP[02]: 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	US DoD ODP Value: at least every 12 months
A.03.06.04.b[01]	Incident Response Training	incident response training content is reviewed <A.03.06.04.ODP[03]: frequency>.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	8	US DoD ODP Value: at least every 12 months
A.03.06.04.b[02]	Incident Response Training	incident response training content is updated <A.03.06.04.ODP[03]: frequency>.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	8	US DoD ODP Value: at least every 12 months
A.03.06.04.b[03]	Incident Response Training	incident response training content is reviewed following <A.03.06.04.ODP[04]: events>.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	8	US DoD ODP Values: (1) at least every 12 months (2) significant, novel incidents, or significant changes to risks
A.03.06.04.b[04]	Incident Response Training	incident response training content is updated following <A.03.06.04.ODP[04]: events>.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	8	US DoD ODP Values: (1) at least every 12 months (2) significant, novel incidents, or significant changes to risks
03.06.05	Incident Response Plan	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.06.05.a.01	Incident Response Plan	an incident response plan is developed that provides the organization with a roadmap for implementing its incident response capability.	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.	5	
A.03.06.05.a.02	Incident Response Plan	an incident response plan is developed that describes the structure and organization of the incident response capability.	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.	5	
A.03.06.05.a.03	Incident Response Plan	an incident response plan is developed that provides a high-level approach for how the incident response capability fits into the overall organization.	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.	5	
A.03.06.05.a.04	Incident Response Plan	an incident response plan is developed that defines reportable incidents.	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.	5	
A.03.06.05.a.05	Incident Response Plan	an incident response plan is developed that addresses the sharing of incident information.	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.	5	
A.03.06.05.a.06	Incident Response Plan	an incident response plan is developed that designates responsibilities to organizational entities, personnel, or roles.	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.	5	
A.03.06.05.b[01]	Incident Response Plan	copies of the incident response plan are distributed to designated incident response personnel (identified by name or by role).	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.	5	
A.03.06.05.b[02]	Incident Response Plan	copies of the incident response plan are distributed to organizational elements.	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.	5	
A.03.06.05.c	Incident Response Plan	the incident response plan is updated 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	
A.03.06.05.d	Incident Response Plan	the incident response plan is protected from unauthorized disclosure.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
A.03.06.05.d	Incident Response Plan	the incident response plan is protected 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.	5	
A.03.06.05.d	Incident Response Plan	the incident response plan is protected 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.	5	
A.03.06.05.d	Incident Response Plan	the incident response plan is protected from unauthorized disclosure.	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	
03.07.01	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.07.02	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.07.03	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.07.04	Maintenance Tools	Determine If:	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
A.03.07.04.a[01]	Maintenance Tools	the use of system maintenance tools is approved.	Functional	Intersects With	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	5	
A.03.07.04.a[02]	Maintenance Tools	the use of system maintenance tools is controlled.	Functional	Intersects With	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	5	
A.03.07.04.a[03]	Maintenance Tools	the use of system maintenance tools is monitored.	Functional	Intersects With	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	5	
A.03.07.04.b	Maintenance Tools	media with diagnostic and test programs are checked for malicious code before the media are used in the system.	Functional	Intersects With	Inspect Media	MNT-04.2	Mechanisms exist to check media containing diagnostic and test programs for malicious code before the media are used.	5	
A.03.07.04.c	Maintenance Tools	the removal of system maintenance equipment containing CUI is prevented 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.	5	
03.07.05	Nonlocal Maintenance	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.07.05.a[01]	Nonlocal Maintenance	nonlocal maintenance and diagnostic activities are approved.	Functional	Intersects With	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	5	
A.03.07.05.a[02]	Nonlocal Maintenance	nonlocal maintenance and diagnostic activities are monitored.	Functional	Intersects With	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	5	
A.03.07.05.b[01]	Nonlocal Maintenance	multi-factor authentication is implemented 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.	5	
A.03.07.05.b[02]	Nonlocal Maintenance	replay resistance is implemented in the establishment of nonlocal maintenance and diagnostic sessions.	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	
A.03.07.05.b[02]	Nonlocal Maintenance	replay resistance is implemented 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.	5	
A.03.07.05.b[02]	Nonlocal Maintenance	replay resistance is implemented 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.	5	
A.03.07.05.c[01]	Nonlocal Maintenance	session connections are terminated 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.	5	
A.03.07.05.c[01]	Nonlocal Maintenance	session connections are terminated 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.	5	
A.03.07.05.c[02]	Nonlocal Maintenance	network connections are terminated when nonlocal maintenance is completed.	Functional	Intersects With	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.	5	
03.07.06	Maintenance Personnel	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.07.06.a	Maintenance Personnel	a process for maintenance personnel authorization is established.	Functional	Intersects With	Authorized Maintenance Personnel	MNT-06	Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.	5	
A.03.07.06.b	Maintenance Personnel	a list of authorized maintenance organizations or personnel is maintained.	Functional	Intersects With	Authorized Maintenance Personnel	MNT-06	Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.	5	
A.03.07.06.c	Maintenance Personnel	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	
A.03.07.06.c	Maintenance Personnel	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	
A.03.07.06.c	Maintenance Personnel	non-escorted personnel who perform maintenance on the system 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.	5	
A.03.07.06.d[01]	Maintenance Personnel	organizational personnel with required access authorizations are designated 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.	5	
A.03.07.06.d[02]	Maintenance Personnel	organizational personnel with required technical competence are designated 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.	5	
03.08.01	Media Storage	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.08.01[01]	Media Storage	system media that contain CUI are physically controlled.	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	
A.03.08.01[02]	Media Storage	system media that contain CUI are securely stored.	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	
03.08.02	Media Access	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.08.02	Media Access	access to CUI on system media is restricted to authorized personnel or roles.	Functional	Intersects With	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	5	
03.08.03	Media Sanitization	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.08.03	Media Sanitization	system media that contain CUI are sanitized 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.	5	
03.08.04	Media Marking	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.08.04[01]	Media Marking	system media that contain CUI are marked to indicate distribution limitations.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
A.03.08.04[02]	Media Marking	system media that contain CUI are marked to indicate handling caveats.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
A.03.08.04[03]	Media Marking	system media that contain CUI are marked to indicate 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.	5	
03.08.05	Media Transport	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.08.05.a[01]	Media Transport	system media that contain CUI are protected 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	
A.03.08.05.a[02]	Media Transport	system media that contain CUI are controlled 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	
A.03.08.05.b	Media Transport	accountability for system media that contain CUI is maintained 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	
A.03.08.05.c	Media Transport	activities associated with the transport of system media that contain CUI are documented.	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	
03.08.06	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.08.07	Media Use	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.08.07.ODP[01]	Media Use	types of system media with usage restrictions or that are prohibited from use are defined.	Functional	Intersects With	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5	
A.03.08.07.a	Media Use	the use of the following types of system media is restricted or prohibited: <A.03.08.07.ODP[01]: types of system media>.	Functional	Intersects With	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	8	US DoD ODP Value: any removable media not managed by or on behalf of the organization
A.03.08.07.b	Media Use	the use of removable system media without an identifiable owner is prohibited.	Functional	Intersects With	Prohibit Use Without Owner	DCH-10.2	Mechanisms exist to prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.	5	
03.08.08	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.08.09	System Backup – Cryptographic Protection	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.08.09.a	System Backup – Cryptographic Protection	the confidentiality of backup information is protected.	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5	
A.03.08.09.b	System Backup – Cryptographic Protection	cryptographic mechanisms are implemented to prevent the unauthorized disclosure of CUI at backup storage locations.	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5	
03.09.01	Personnel Screening	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.09.01.ODP[01]	Personnel Screening	conditions that require the rescreening of individuals are defined.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
A.03.09.01.ODP[01]	Personnel Screening	conditions that require the rescreening of individuals are defined.	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	
A.03.09.01.a	Personnel Screening	individuals are screened prior to authorizing access to the system.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
A.03.09.01.b	Personnel Screening	individuals are rescreened in accordance with the following conditions: <A.03.09.01.ODP[01]: conditions>.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	8	US DoD ODP Value: an organizational policy requiring rescreening when there is a significant incident, or change in status, related to an individual
03.09.02	Personnel Termination and Transfer	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.09.02.ODP[01]	Personnel Termination and Transfer	the time period within which to disable system access is defined.	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	
A.03.09.02.ODP[01]	Personnel Termination and Transfer	the time period within which to disable system access is defined.	Functional	Intersects With	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	
A.03.09.02.a.01	Personnel Termination and Transfer	upon termination of individual employment, system access is disabled within <A.03.09.02.ODP[01]: time period>.	Functional	Intersects With	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	8	US DoD ODP Value: four (4) hours
A.03.09.02.a.02[01]	Personnel Termination and Transfer	upon termination of individual employment, authenticators associated with the individual are terminated or revoked.	Functional	Intersects With	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	
A.03.09.02.a.02[02]	Personnel Termination and Transfer	upon termination of individual employment, credentials associated with the individual are terminated or revoked.	Functional	Intersects With	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	
A.03.09.02.a.03	Personnel Termination and Transfer	upon termination of individual employment, security-related system property is retrieved.	Functional	Intersects With	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.	5	
A.03.09.02.a.03	Personnel Termination and Transfer	upon termination of individual employment, security-related system property is retrieved.	Functional	Intersects With	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	
A.03.09.02.a.03	Personnel Termination and Transfer	upon termination of individual employment, security-related system property is retrieved.	Functional	Intersects With	Asset Collection	HRS-09.1	Mechanisms exist to retrieve organization-owned assets upon termination of an individual's employment.	5	
A.03.09.02.b.01[01]	Personnel Termination and Transfer	upon individual reassignment or transfer to other positions in the organization, the ongoing operational need for current logical and physical access authorizations to the system and facility is reviewed.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
A.03.09.02.b.01[01]	Personnel Termination and Transfer	upon individual reassignment or transfer to other positions in the organization, the ongoing operational need for current logical and physical access authorizations to the system and facility is reviewed.	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	
A.03.09.02.b.01[02]	Personnel Termination and Transfer	upon individual reassignment or transfer to other positions in the organization, the ongoing operational need for current logical and physical access authorizations to the system and facility is confirmed.	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	
A.03.09.02.b.02	Personnel Termination and Transfer	upon individual reassignment or transfer to other positions in the organization, access authorization is modified to correspond with any changes in operational need.	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	
03.10.01	Physical Access Authorizations	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.10.01.ODP[01]	Physical Access Authorizations	the frequency at which to review the access list detailing authorized facility access by individuals is defined.	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	
A.03.10.01.ODP[01]	Physical Access Authorizations	the frequency at which to review the access list detailing authorized facility access by individuals is defined.	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	
A.03.10.01.a[01]	Physical Access Authorizations	a list of individuals with authorized access to the facility where the system resides is developed.	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	
A.03.10.01.a[02]	Physical Access Authorizations	a list of individuals with authorized access to the facility where the system resides is approved.	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	
A.03.10.01.a[03]	Physical Access Authorizations	a list of individuals with authorized access to the facility where the system resides is maintained.	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	
A.03.10.01.b	Physical Access Authorizations	authorization credentials for facility access are issued.	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	
A.03.10.01.c	Physical Access Authorizations	the facility access list is reviewed <A.03.10.01.ODP[01]: 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	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
A.03.10.01.d	Physical Access Authorizations	individuals from the facility access list are removed 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).	5	
03.10.02	Monitoring Physical Access	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.10.02.ODP[01]	Monitoring Physical Access	the frequency at which to review physical access logs is defined.	Functional	Intersects With	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5	
A.03.10.02.ODP[02]	Monitoring Physical Access	events or potential indications of events requiring physical access logs to be reviewed are defined.	Functional	Intersects With	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5	
A.03.10.02.a[01]	Monitoring Physical Access	physical access to the facility where the system resides is monitored to detect physical security incidents.	Functional	Intersects With	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5	
A.03.10.02.a[02]	Monitoring Physical Access	physical security incidents are responded to.	Functional	Intersects With	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5	
A.03.10.02.b[01]	Monitoring Physical Access	physical access logs are reviewed <A.03.10.02.ODP[01]: frequency>.	Functional	Intersects With	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	8	US DoD ODP Values: at least every 45 days
A.03.10.02.b[02]	Monitoring Physical Access	physical access logs are reviewed upon occurrence of <A.03.10.02.ODP[02]: events or potential indicators of events>.	Functional	Intersects With	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	8	US DoD ODP Values: significant, novel incidents, or significant changes to risks.
03.10.03	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.10.04	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.10.05	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.10.06	Alternate Work Site	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.10.06.ODP[01]	Alternate Work Site	security requirements to be employed at alternate work sites are defined.	Functional	Intersects With	Alternate Work Site	PES-11	Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.	5	
A.03.10.06.ODP[01]	Alternate Work Site	security requirements to be employed at alternate work sites are defined.	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	
A.03.10.06.a	Alternate Work Site	alternate work sites allowed for use by employees are determined.	Functional	Intersects With	Alternate Work Site	PES-11	Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.	5	
A.03.10.06.a	Alternate Work Site	alternate work sites allowed for use by employees are determined.	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	
A.03.10.06.b	Alternate Work Site	the following security requirements are employed at alternate work sites: <A.03.10.06.ODP[01]: 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	US DoD ODP Value: adequate security, comparable to organizational security requirements at the primary work site where practical, documented in policy, and covered by training
A.03.10.06.b	Alternate Work Site	the following security requirements are employed at alternate work sites: <A.03.10.06.ODP[01]: 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	US DoD 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	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.10.07.a.01	Physical Access Control	physical access authorizations are enforced at entry and exit points to the facility where the system resides by verifying individual physical access authorizations before granting 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	
A.03.10.07.a.02	Physical Access Control	physical access authorizations are enforced at entry and exit points to the facility where the system resides by controlling ingress and egress with physical access control systems, devices, or guards.	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	
A.03.10.07.b	Physical Access Control	physical access audit logs for entry or exit points are maintained.	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.	5	
A.03.10.07.c[01]	Physical Access Control	visitors are escorted.	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	
A.03.10.07.c[01]	Physical Access Control	visitors are escorted.	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	
A.03.10.07.c[01]	Physical Access Control	visitors are escorted.	Functional	Intersects With	Restrict Unescorted Access	PES-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.	5	
A.03.10.07.c[02]	Physical Access Control	visitor activity is controlled.	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	
A.03.10.07.c[02]	Physical Access Control	visitor activity is controlled.	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	
A.03.10.07.c[02]	Physical Access Control	visitor activity is controlled.	Functional	Intersects With	Restrict Unescorted Access	PES-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.	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
A.03.10.07.d	Physical Access Control	keys, combinations, and other physical access devices are secured.	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	
A.03.10.07.e	Physical Access Control	physical access to output devices is controlled to prevent unauthorized individuals from obtaining access to CUI.	Functional	Intersects With	Access Control for Output Devices	PES-12.2	Physical security mechanisms exist to restrict access to printers and other system output devices to prevent unauthorized individuals from obtaining the output.	5	
03.10.08	Access Control for Transmission	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.10.08	Access Control for Transmission	physical access to system distribution and transmission lines within organizational facilities is controlled.	Functional	Intersects With	Transmission Medium Security	PES-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	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.11.01.ODP[01]	Risk Assessment	the frequency at which to update the risk assessment is defined.	Functional	Intersects With	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.	5	
A.03.11.01.a	Risk Assessment	the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI is assessed.	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
A.03.11.01.a	Risk Assessment	the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI is assessed.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
A.03.11.01.a	Risk Assessment	the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI is assessed.	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.	5	
A.03.11.01.a	Risk Assessment	the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI is assessed.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
A.03.11.01.a	Risk Assessment	the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI is assessed.	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	
A.03.11.01.b	Risk Assessment	risk assessments are updated <A.03.11.01.ODP[01]: frequency>.	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	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
A.03.11.01.b	Risk Assessment	risk assessments are updated <A.03.11.01.ODP[01]: frequency>.	Functional	Intersects With	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.	8	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
03.11.02	Vulnerability Monitoring and Scanning	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.11.02.ODP[01]	Vulnerability Monitoring and Scanning	the frequency at which the system is monitored for vulnerabilities is defined.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
A.03.11.02.ODP[02]	Vulnerability Monitoring and Scanning	the frequency at which the system is scanned for vulnerabilities is defined.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
A.03.11.02.ODP[03]	Vulnerability Monitoring and Scanning	response times to remediate system vulnerabilities are defined.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
A.03.11.02.ODP[03]	Vulnerability Monitoring and Scanning	response times to remediate system vulnerabilities are defined.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
A.03.11.02.ODP[04]	Vulnerability Monitoring and Scanning	the frequency at which to update system vulnerabilities to be scanned is defined.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
A.03.11.02.ODP[04]	Vulnerability Monitoring and Scanning	the frequency at which to update system vulnerabilities to be scanned is defined.	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5	
A.03.11.02.a[01]	Vulnerability Monitoring and Scanning	the system is monitored for vulnerabilities <A.03.11.02.ODP[01]: frequency>.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	8	US DoD ODP Value: at least monthly, or when there are significant incidents or significant changes to risks
A.03.11.02.a[01]	Vulnerability Monitoring and Scanning	the system is monitored for vulnerabilities <A.03.11.02.ODP[01]: frequency>.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	8	US DoD ODP Value: at least monthly, or when there are significant incidents or significant changes to risks
A.03.11.02.a[02]	Vulnerability Monitoring and Scanning	the system is scanned for vulnerabilities <A.03.11.02.ODP[02]: frequency>.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	8	US DoD ODP Value: at least monthly, or when there are significant incidents or significant changes to risks
A.03.11.02.a[03]	Vulnerability Monitoring and Scanning	the system is monitored for vulnerabilities when new vulnerabilities that affect the system are identified.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
A.03.11.02.a[04]	Vulnerability Monitoring and Scanning	the system is scanned for vulnerabilities when new vulnerabilities that affect the system are identified.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
A.03.11.02.b	Vulnerability Monitoring and Scanning	system vulnerabilities are remediated within <A.03.11.02.ODP[03]: 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	US DoD 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
A.03.11.02.b	Vulnerability Monitoring and Scanning	system vulnerabilities are remediated within <A.03.11.02.ODP[03]: 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	US DoD 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
A.03.11.02.c[01]	Vulnerability Monitoring and Scanning	system vulnerabilities to be scanned are updated <A.03.11.02.ODP[04]: frequency>.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	8	US DoD ODP Value: no more than 24 hours prior to running the scans
A.03.11.02.c[01]	Vulnerability Monitoring and Scanning	system vulnerabilities to be scanned are updated <A.03.11.02.ODP[04]: frequency>.	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	8	US DoD ODP Value: no more than 24 hours prior to running the scans
A.03.11.02.c[02]	Vulnerability Monitoring and Scanning	system vulnerabilities to be scanned are updated when new vulnerabilities are identified and reported.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
A.03.11.02.c[02]	Vulnerability Monitoring and Scanning	system vulnerabilities to be scanned are updated when new vulnerabilities are identified and reported.	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	5	
03.11.03	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.11.04	Risk Response	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.11.04[01]	Risk Response	findings from security assessments are responded to.	Functional	Intersects With	Risk Response	RSK-06.1	[illegible] performed to remediate findings from security, compliance and/or resilience-related: (1) Assessments; (2) Audits; and/or	5	
A.03.11.04[02]	Risk Response	findings from security monitoring are responded to.	Functional	Intersects With	Risk Response	RSK-06.1	[illegible] performed to remediate findings from security, compliance and/or resilience-related: (1) Assessments; (2) Audits; and/or	5	
A.03.11.04[03]	Risk Response	findings from security audits are responded to.	Functional	Intersects With	Risk Response	RSK-06.1	[illegible] performed to remediate findings from security, compliance and/or resilience-related: (1) Assessments; (2) Audits; and/or	5	
03.12.01	Security Assessment	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.12.01.ODP[01]	Security Assessment	the frequency at which to assess the security requirements for the system and its environment of operation is defined.	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.	5	
A.03.12.01	Security Assessment	the security requirements for the system and its environment of operation are assessed <A.03.12.01.ODP[01]: 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	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
03.12.02	Plan of Action and Milestones	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.12.02.a.01	Plan of Action and Milestones	a plan of action and milestones for the system is developed to document the planned remediation actions for correcting weaknesses or deficiencies noted during security assessments.	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., asset/process owner);	5	
A.03.12.02.a.02	Plan of Action and Milestones	a plan of action and milestones for the system is developed to reduce or eliminate known system vulnerabilities.	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., 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
A.03.12.02.b.01	Plan of Action and Milestones	the existing plan of action and milestones is updated based on the findings from security assessments.	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., asset/process owner);	5	
A.03.12.02.b.02	Plan of Action and Milestones	the existing plan of action and milestones is updated based on the findings from audits or reviews.	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., asset/process owner);	5	
A.03.12.02.b.03	Plan of Action and Milestones	the existing plan of action and milestones is updated based on the findings from continuous monitoring activities.	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., asset/process owner);	5	
03.12.03	Continuous Monitoring	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.12.03[01]	Continuous Monitoring	a system-level continuous monitoring strategy is developed.	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	
A.03.12.03[02]	Continuous Monitoring	a system-level continuous monitoring strategy is implemented.	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	
A.03.12.03[03]	Continuous Monitoring	ongoing monitoring is included in the continuous monitoring strategy.	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	
A.03.12.03[04]	Continuous Monitoring	security assessments are included in the continuous monitoring strategy.	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	
03.12.04	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.12.05	Information Exchange	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.12.05.ODP[01]	Information Exchange	one or more of the following PARAMETER VALUES are selected: {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	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	
A.03.12.05.ODP[02]	Information Exchange	the frequency at which to review and update agreements is defined.	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	
A.03.12.05.a[01]	Information Exchange	the exchange of CUI between the system and other systems is approved using <A.03.12.05.ODP[01]: SELECTED PARAMETER VALUES>.	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	US DoD ODP Value: requirements as described in the contract
A.03.12.05.a[02]	Information Exchange	the exchange of CUI between the system and other systems is managed using <A.03.12.05.ODP[01]: SELECTED PARAMETER VALUES>.	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	US DoD ODP Value: requirements as described in the contract
A.03.12.05.b[01]	Information Exchange	interface characteristics for each system are documented 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.	5	
A.03.12.05.b[02]	Information Exchange	security requirements for each system are documented 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.	5	
A.03.12.05.b[03]	Information Exchange	responsibilities for each system are documented 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.	5	
A.03.12.05.c[01]	Information Exchange	exchange agreements are reviewed <A.03.12.05.ODP[02]: frequency>.	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	US DoD ODP Value: at least every 12 months
A.03.12.05.c[02]	Information Exchange	exchange agreements are updated <A.03.12.05.ODP[02]: frequency>.	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	US DoD ODP Value: at least every 12 months
03.13.01	Boundary Protection	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.13.01.a[01]	Boundary Protection	communications at external managed interfaces to the system are monitored.	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.	5	
A.03.13.01.a[02]	Boundary Protection	communications at external managed interfaces to the system are controlled.	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	
A.03.13.01.a[03]	Boundary Protection	communications at key internal managed interfaces within the system are monitored.	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.	5	
A.03.13.01.a[04]	Boundary Protection	communications at key internal managed interfaces within the system are controlled.	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	
A.03.13.01.b	Boundary Protection	subnetworks are implemented for publicly accessible system components that are physically or logically separated from internal networks.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	5	
A.03.13.01.c	Boundary Protection	external system connections are only made 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	
03.13.02	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.13.03	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.13.04	Information in Shared System Resources	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.13.04[01]	Information in Shared System Resources	unauthorized information transfer via shared system resources is prevented.	Functional	Intersects With	Information In Shared Resources	SEA-05	Mechanisms exist to prevent unauthorized and unintended information transfer via shared system resources.	5	
A.03.13.04[02]	Information in Shared System Resources	unintended information transfer via shared system resources is prevented.	Functional	Intersects With	Information In Shared Resources	SEA-05	Mechanisms exist to prevent unauthorized and unintended information transfer via shared system resources.	5	
03.13.05	Withdrawn	N/A	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	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.13.06[01]	Network Communications – Deny by Default – Allow by Exception	network communications traffic is denied by default.	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	
A.03.13.06[02]	Network Communications – Deny by Default – Allow by Exception	network communications traffic is allowed by exception.	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	
03.13.07	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.13.08	Transmission and Storage Confidentiality	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.13.08[01]	Transmission and Storage Confidentiality	cryptographic mechanisms are implemented to prevent the unauthorized disclosure of CUI during transmission.	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	
A.03.13.08[01]	Transmission and Storage Confidentiality	cryptographic mechanisms are implemented to prevent the unauthorized disclosure of CUI during transmission.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
A.03.13.08[02]	Transmission and Storage Confidentiality	cryptographic mechanisms are implemented to prevent the unauthorized disclosure of CUI 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	
A.03.13.08[02]	Transmission and Storage Confidentiality	cryptographic mechanisms are implemented to prevent the unauthorized disclosure of CUI while in storage.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
03.13.09	Network Disconnect	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.13.09.ODP[01]	Network Disconnect	the time period of inactivity after which the system terminates a network connection associated with a communications session is defined.	Functional	Intersects With	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.	5	
A.03.13.09	Network Disconnect	the network connection associated with a communications session is terminated at the end of the session or after <A.03.13.09.ODP[01]: time period> of inactivity.	Functional	Intersects With	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.	8	US DoD ODP Value: no longer than 15 minutes

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
03.13.10	Cryptographic Key Establishment and Management	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.13.10.ODP[01]	Cryptographic Key Establishment and Management	requirements for key generation, distribution, storage, access, and destruction are defined.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
A.03.13.10[01]	Cryptographic Key Establishment and Management	cryptographic keys are established in the system in accordance with the following key management requirements: <A.03.13.10.ODP[01]: requirements>.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	8	US DoD ODP Value: Guidance: At a minimum, establish a policy and procedure in line with the latest Cryptographic key management guidance
A.03.13.10[02]	Cryptographic Key Establishment and Management	cryptographic keys are managed in the system in accordance with the following key management requirements: <A.03.13.10.ODP[01]: requirements>.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	8	US DoD ODP Value: Guidance: At a minimum, establish a policy and procedure in line with the latest Cryptographic key management guidance
03.13.11	Cryptographic Protection	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.13.11.ODP[01]	Cryptographic Protection	the types of cryptography for protecting the confidentiality of CUI are defined.	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	
A.03.13.11.ODP[01]	Cryptographic Protection	the types of cryptography for protecting the confidentiality of CUI are defined.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
A.03.13.11.ODP[01]	Cryptographic Protection	the types of cryptography for protecting the confidentiality of CUI are defined.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
A.03.13.11	Cryptographic Protection	the following types of cryptography are implemented to protect the confidentiality of CUI: <A.03.13.11.ODP[01]: 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	US DoD ODP Value: FIPS Validated Cryptography (https://csrc.nist.gov/Projects/Cryptographic-ModuleValidation-Program/Validated-Modules)
A.03.13.11	Cryptographic Protection	the following types of cryptography are implemented to protect the confidentiality of CUI: <A.03.13.11.ODP[01]: types of cryptography>.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	8	US DoD ODP Value: FIPS Validated Cryptography (https://csrc.nist.gov/Projects/Cryptographic-ModuleValidation-Program/Validated-Modules)
A.03.13.11	Cryptographic Protection	the following types of cryptography are implemented to protect the confidentiality of CUI: <A.03.13.11.ODP[01]: types of cryptography>.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	8	US DoD ODP Value: FIPS Validated Cryptography (https://csrc.nist.gov/Projects/Cryptographic-ModuleValidation-Program/Validated-Modules)
03.13.12	Collaborative Computing Devices and Applications	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.13.12.ODP[01]	Collaborative Computing Devices and Applications	exceptions where remote activation is to be allowed are defined.	Functional	Intersects With	Collaborative Computing Devices	END-14	Mechanisms exist to unplug or prohibit the remote activation of collaborative computing devices with the following exceptions: (1) Networked whiteboards; (2) Video teleconference cameras; and (3) Teleconference microphones.	5	
A.03.13.12.a	Collaborative Computing Devices and Applications	the remote activation of collaborative computing devices and applications is prohibited with the following exceptions: <A.03.13.12.ODP[01]: exceptions>.	Functional	Intersects With	Collaborative Computing Devices	END-14	Mechanisms exist to unplug or prohibit the remote activation of collaborative computing devices with the following exceptions: (1) Networked whiteboards; (2) Video teleconference cameras; and (3) Teleconference microphones.	8	US DoD 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
A.03.13.12.b	Collaborative Computing Devices and Applications	an explicit indication of use is provided to users who are physically present at the devices.	Functional	Intersects With	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.	5	
03.13.13	Mobile Code	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.13.13.a[01]	Mobile Code	acceptable mobile code is defined.	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
A.03.13.13.a[02]	Mobile Code	acceptable mobile code technologies are defined.	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
A.03.13.13.b[01]	Mobile Code	the use of mobile code is authorized.	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
A.03.13.13.b[02]	Mobile Code	the use of mobile code is monitored.	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
A.03.13.13.b[03]	Mobile Code	the use of mobile code is controlled.	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	
A.03.13.13.b[03]	Mobile Code	the use of mobile code is controlled.	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
03.13.14	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.13.15	Session Authenticity	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.13.15	Session Authenticity	the authenticity of communications sessions is protected.	Functional	Intersects With	Session Integrity	NET-09	Mechanisms exist to protect the authenticity and integrity of communications sessions.	5	
03.13.16	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.14.01	Flaw Remediation	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.14.01.ODP[01]	Flaw Remediation	the time period within which to install security-relevant software updates after the release of the updates is defined.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
A.03.14.01.ODP[02]	Flaw Remediation	the time period within which to install security-relevant firmware updates after the release of the updates is defined.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
A.03.14.01.a[01]	Flaw Remediation	system flaws are identified.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
A.03.14.01.a[02]	Flaw Remediation	system flaws are reported.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
A.03.14.01.a[03]	Flaw Remediation	system flaws are corrected.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
A.03.14.01.b[01]	Flaw Remediation	security-relevant software updates are installed within <A.03.14.01.ODP[01]: 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	US DoD 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
A.03.14.01.b[02]	Flaw Remediation	security-relevant firmware updates are installed within <A.03.14.01.ODP[02]: 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	US DoD 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	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.14.02.ODP[01]	Malicious Code Protection	the frequency at which malicious code protection mechanisms perform scans is defined.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
A.03.14.02.a[01]	Malicious Code Protection	malicious code protection mechanisms are implemented at system entry and exit points to detect malicious code.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
A.03.14.02.a[02]	Malicious Code Protection	malicious code protection mechanisms are implemented at system entry and exit points to eradicate malicious code.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
A.03.14.02.b	Malicious Code Protection	malicious code protection mechanisms are updated as new releases are available in accordance with configuration management policy and procedures.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5	
A.03.14.02.c.01[01]	Malicious Code Protection	malicious code protection mechanisms are configured to perform scans of the system <A.03.14.02.ODP[01]: frequency>.	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	US DoD ODP Value: at least weekly
A.03.14.02.c.01[02]	Malicious Code Protection	malicious code protection mechanisms are configured to perform real-time scans of files from external sources at endpoints or system entry and exit points as the files are downloaded, opened, or executed.	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	
A.03.14.02.c.02	Malicious Code Protection	malicious code protection mechanisms are configured to block malicious code, quarantine malicious code, or take other 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.	5	
03.14.03	Security Alerts, Advisories, and Directives	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.14.03.a	Security Alerts, Advisories, and Directives	system security alerts, advisories, and directives from external organizations are received 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	
A.03.14.03.b[01]	Security Alerts, Advisories, and Directives	internal security alerts, advisories, and directives are generated, as necessary.	Functional	Intersects With	Threat Intelligence Reporting	THR-03.1	Mechanisms exist to utilize external threat intelligence feeds to generate and disseminate organization-specific security alerts, advisories and/or directives.	5	
A.03.14.03.b[02]	Security Alerts, Advisories, and Directives	internal security alerts, advisories, and directives are disseminated, as necessary.	Functional	Intersects With	Threat Intelligence Reporting	THR-03.1	Mechanisms exist to utilize external threat intelligence feeds to generate and disseminate organization-specific security alerts, advisories and/or directives.	5	
03.14.04	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.14.05	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.14.06	System Monitoring	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.14.06.a.01[01]	System Monitoring	the system is monitored to detect attacks.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
A.03.14.06.a.01[02]	System Monitoring	the system is monitored to detect indicators of potential attacks.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
A.03.14.06.a.02	System Monitoring	the system is monitored to detect unauthorized connections.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
A.03.14.06.b	System Monitoring	unauthorized use of the system is identified.	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.	5	
A.03.14.06.c[01]	System Monitoring	inbound communications traffic is monitored 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.	5	
A.03.14.06.c[02]	System Monitoring	outbound communications traffic is monitored 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.	5	
03.14.07	Withdrawn	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
03.14.08	Information Management and Retention	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.14.08[01]	Information Management and Retention	CUI within the system is managed in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
A.03.14.08[02]	Information Management and Retention	CUI within the system is retained in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
A.03.14.08[03]	Information Management and Retention	CUI output from the system is managed in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
A.03.14.08[04]	Information Management and Retention	CUI output from the system is retained in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
03.15.01	Policy and Procedures	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.15.01.ODP[01]	Policy and Procedures	the frequency at which the policies and procedures for satisfying security requirements are reviewed and updated is defined.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
A.03.15.01.a[01]	Policy and Procedures	policies needed to satisfy the security requirements for the protection of CUI are developed and documented.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
A.03.15.01.a[02]	Policy and Procedures	policies needed to satisfy the security requirements for the protection of CUI are disseminated to organizational personnel or roles.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
A.03.15.01.a[03]	Policy and Procedures	procedures needed to satisfy the security requirements for the protection of CUI are developed and documented.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
A.03.15.01.a[03]	Policy and Procedures	procedures needed to satisfy the security requirements for the protection of CUI are developed and documented.	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.	5	
A.03.15.01.a[04]	Policy and Procedures	procedures needed to satisfy the security requirements for the protection of CUI are disseminated to organizational personnel or roles.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
A.03.15.01.a[04]	Policy and Procedures	procedures needed to satisfy the security requirements for the protection of CUI are disseminated to organizational personnel or roles.	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.	5	
A.03.15.01.b[01]	Policy and Procedures	policies and procedures are reviewed <A.03.15.01.ODP[01]: 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	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
A.03.15.01.b[01]	Policy and Procedures	policies and procedures are reviewed <A.03.15.01.ODP[01]: frequency>.	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	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
A.03.15.01.b[02]	Policy and Procedures	policies and procedures are updated <A.03.15.01.ODP[01]: 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	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
A.03.15.01.b[02]	Policy and Procedures	policies and procedures are updated <A.03.15.01.ODP[01]: frequency>.	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	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
03.15.02	System Security Plan	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.15.02.ODP[01]	System Security Plan	the frequency at which the system security plan is reviewed and updated is defined.	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: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system	10	
A.03.15.02.a.01	System Security Plan	a system security plan that defines the constituent system components is developed.	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: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system	10	
A.03.15.02.a.02	System Security Plan	a system security plan that identifies the information types processed, stored, and transmitted by the system is developed.	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: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system	10	
A.03.15.02.a.03	System Security Plan	a system security plan that describes specific threats to the system that are of concern to the organization is developed.	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: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system	10	
A.03.15.02.a.04	System Security Plan	a system security plan that describes the operational environment for the system and any dependencies on or connections to other systems or system components is developed.	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: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system	10	
A.03.15.02.a.05	System Security Plan	a system security plan that provides an overview of the security requirements for the system is developed.	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: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system	10	
A.03.15.02.a.06	System Security Plan	a system security plan that describes the safeguards in place or planned for meeting the security requirements is developed.	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: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system	10	
A.03.15.02.a.07	System Security Plan	a system security plan that identifies individuals that fulfill system roles and responsibilities is developed.	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: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system	10	
A.03.15.02.a.08	System Security Plan	a system security plan that includes other relevant information necessary for the protection of CUI is developed.	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: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system	10	
A.03.15.02.b[01]	System Security Plan	the system security plan is reviewed <A.03.15.02.ODP[01]: 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: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system	10	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
A.03.15.02.b[02]	System Security Plan	the system security plan is updated <A.03.15.02.ODP[01]: 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: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system	10	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
A.03.15.02.c	System Security Plan	the system security plan is protected 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.	5	
A.03.15.02.c	System Security Plan	the system security plan is protected 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.	5	
A.03.15.02.c	System Security Plan	the system security plan is protected from unauthorized disclosure.	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: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system	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	Rules of Behavior	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.15.03.ODP[01]	Rules of Behavior	the frequency at which the rules of behavior are reviewed and updated is defined.	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	
A.03.15.03.a	Rules of Behavior	rules that describe responsibilities and expected behavior for system usage and protecting CUI are established.	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	
A.03.15.03.a	Rules of Behavior	rules that describe responsibilities and expected behavior for system usage and protecting CUI are established.	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.	5	
A.03.15.03.a	Rules of Behavior	rules that describe responsibilities and expected behavior for system usage and protecting CUI are established.	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	
A.03.15.03.a	Rules of Behavior	rules that describe responsibilities and expected behavior for system usage and protecting CUI are established.	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	
A.03.15.03.b	Rules of Behavior	rules are provided to individuals who require access to the system.	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	
A.03.15.03.c	Rules of Behavior	a documented acknowledgement from individuals indicating that they have read, understand, and agree to abide by the rules of behavior is received before authorizing access to CUI and the system.	Functional	Intersects With	Policy Familiarization & Acknowledgement	HRS-05.7	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's security, compliance and resilience policies and provide acknowledgement.	5	
A.03.15.03.d[01]	Rules of Behavior	the rules of behavior are reviewed <A.03.15.03.ODP[01]: frequency>.	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.	8	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
A.03.15.03.d[02]	Rules of Behavior	the rules of behavior are updated <A.03.15.03.ODP[01]: frequency>.	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.	8	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
03.16.01	Security Engineering Principles	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.16.01.ODP[01]	Security Engineering Principles	systems security engineering principles to be applied to the development or modification of the system and system components are defined.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
A.03.16.01.ODP[01]	Security Engineering Principles	systems security engineering principles to be applied to the development or modification of the system and system components are defined.	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
A.03.16.01.ODP[01]	Security Engineering Principles	systems security engineering principles to be applied to the development or modification of the system and system components are defined.	Functional	Subset Of	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	10	
A.03.16.01	Security Engineering Principles	<A.03.16.01.ODP[01]: systems security engineering principles> are applied to the development or modification of the system and system components.	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.	5	US DoD 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.
A.03.16.01	Security Engineering Principles	<A.03.16.01.ODP[01]: systems security engineering principles> are applied to the development or modification of the system and system components.	Functional	Subset Of	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	10	US DoD 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.
03.16.02	Unsupported System Components	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.16.02.a	Unsupported System Components	system components are replaced when support for the components is no longer available from the developer, vendor, or manufacturer.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	TDA-17	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (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.	5	
A.03.16.02.b	Unsupported System Components	options for risk mitigation or alternative sources for continued support for unsupported components that cannot be replaced are provided.	Functional	Intersects With	Alternate Sources for Continued Support	TDA-17.1	Mechanisms exist to provide in-house support or contract external providers for support with unsupported Technology Assets, Applications and/or Services (TAAS).	5	
03.16.03	External System Services	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.16.03.ODP[01]	External System Services	security requirements to be satisfied by external system service providers are defined.	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	
A.03.16.03.ODP[01]	External System Services	security requirements to be satisfied by external system service providers are defined.	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	
A.03.16.03.a	External System Services	the providers of external system services used for the processing, storage, or transmission of CUI comply with the following security requirements: <A.03.16.03.ODP[01]: 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	US DoD ODP Values: (1) For cloud service providers: (i) FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline in accordance with the FedRAMP Marketplace; or (ii) meets security requirements established by the government equivalent to the FedRAMP Moderate (or higher) baseline. (2) All other external service providers must meet NIST SP 800-171 R2.
A.03.16.03.b	External System Services	user roles and responsibilities with regard to external system services, including shared responsibilities with external service providers, are defined and documented.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5	
A.03.16.03.c	External System Services	processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis are implemented.	Functional	Intersects With	Third-Party Scope Review	TPM-05.5	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure security, compliance and resilience control assignments accurately reflect current: (1) Contractual obligations for the External Service Provider (ESP); (2) Business practices; (3) Applicable stakeholders; and (4) Deployed Technology Assets, Applications and/or Services	5	
A.03.16.03.c	External System Services	processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis are implemented.	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.	5	
A.03.16.03.c	External System Services	processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis are implemented.	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.	5	
A.03.16.03.c	External System Services	processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis are implemented.	Functional	Intersects With	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.	5	
03.17.01	Supply Chain Risk Management Plan	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.17.01.ODP[01]	Supply Chain Risk Management Plan	the frequency at which to review and update the supply chain risk management plan is defined.	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	

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
A.03.17.01.a[01]	Supply Chain Risk Management Plan	a plan for managing supply chain risks is developed.	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	
A.03.17.01.a[02]	Supply Chain Risk Management Plan	the SCRM plan addresses risks associated with the research and development of the system, system components, or system services.	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	
A.03.17.01.a[03]	Supply Chain Risk Management Plan	the SCRM plan addresses risks associated with the design of the system, system components, or system services.	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	
A.03.17.01.a[04]	Supply Chain Risk Management Plan	the SCRM plan addresses risks associated with the manufacturing of the system, system components, or system services.	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	
A.03.17.01.a[05]	Supply Chain Risk Management Plan	the SCRM plan addresses risks associated with the acquisition of the system, system components, or system services.	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	
A.03.17.01.a[06]	Supply Chain Risk Management Plan	the SCRM plan addresses risks associated with the delivery of the system, system components, or system services.	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	
A.03.17.01.a[07]	Supply Chain Risk Management Plan	the SCRM plan addresses risks associated with the integration of the system, system components, or system services.	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	
A.03.17.01.a[08]	Supply Chain Risk Management Plan	the SCRM plan addresses risks associated with the operation of the system, system components, or system services.	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	
A.03.17.01.a[09]	Supply Chain Risk Management Plan	the SCRM plan addresses risks associated with the maintenance of the system, system components, or system services.	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	
A.03.17.01.a[10]	Supply Chain Risk Management Plan	the SCRM plan addresses risks associated with the disposal of the system, system components, or system services.	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	
A.03.17.01.b[01]	Supply Chain Risk Management Plan	the SCRM plan is reviewed <A.03.17.01.ODP[01]: 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	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
A.03.17.01.b[02]	Supply Chain Risk Management Plan	the SCRM plan is updated <A.03.17.01.ODP[01]: 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	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
A.03.17.01.c	Supply Chain Risk Management Plan	the SCRM plan is protected 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.	5	
A.03.17.01.c	Supply Chain Risk Management Plan	the SCRM plan is protected 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.	5	
A.03.17.01.c	Supply Chain Risk Management Plan	the SCRM plan is protected from unauthorized disclosure.	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	
03.17.02	Acquisition Strategies, Tools, and Methods	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.17.02[01]	Acquisition Strategies, Tools, and Methods	acquisition strategies, contract tools, and procurement methods are developed to identify supply chain risks.	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	
A.03.17.02[02]	Acquisition Strategies, Tools, and Methods	acquisition strategies, contract tools, and procurement methods are developed to protect against supply chain risks.	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	
A.03.17.02[03]	Acquisition Strategies, Tools, and Methods	acquisition strategies, contract tools, and procurement methods are developed to mitigate supply chain risks.	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	
A.03.17.02[04]	Acquisition Strategies, Tools, and Methods	acquisition strategies, contract tools, and procurement methods are implemented to identify 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	
A.03.17.02[05]	Acquisition Strategies, Tools, and Methods	acquisition strategies, contract tools, and procurement methods are implemented to protect against 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	
A.03.17.02[06]	Acquisition Strategies, Tools, and Methods	acquisition strategies, contract tools, and procurement methods are implemented to 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	
03.17.03	Supply Chain Requirements and Processes	Determine If:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
A.03.17.03.ODP[01]	Supply Chain Requirements and Processes	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 are defined.	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	
A.03.17.03.ODP[01]	Supply Chain Requirements and Processes	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 are defined.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
A.03.17.03.a[01]	Supply Chain Requirements and Processes	a process for identifying weaknesses or deficiencies in the supply chain elements and processes is established.	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	
A.03.17.03.a[01]	Supply Chain Requirements and Processes	a process for identifying weaknesses or deficiencies in the supply chain elements and processes is established.	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	
A.03.17.03.a[02]	Supply Chain Requirements and Processes	a process for addressing weaknesses or deficiencies in the supply chain elements and processes is established.	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	
A.03.17.03.b	Supply Chain Requirements and Processes	the following security requirements are enforced to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences of supply chain-related events: <A.03.17.03.ODP[01]: security requirements>.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	US DoD 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
A.03.17.03.b	Supply Chain Requirements and Processes	the following security requirements are enforced to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences of supply chain-related events: <A.03.17.03.ODP[01]: 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	US DoD 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

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
N/A	N/A	N/A	N/A	N/A
YES	E-HRS-01 E-HRS-15 E-HRS-27	HRS-01_A29	the time period for account inactivity before disabling is defined.	
YES		IAC-15_A47	the time period for account inactivity before disabling is defined.	
YES	E-HRS-01 E-HRS-15 E-HRS-27	HRS-01_A30	the time period within which to notify account managers and designated personnel or roles when accounts are no longer required is defined.	
YES	E-HRS-01 E-HRS-15 E-HRS-27	HRS-01_A31	the time period within which to notify account managers and designated personnel or roles when users are terminated or transferred is defined.	
YES	E-HRS-01 E-HRS-15 E-HRS-27	HRS-01_A32	the time period within which to notify account managers and designated personnel or roles when system usage or the need-to-know changes for an individual is defined.	
		IAC-25_A04	the time period of expected inactivity requiring users to log out of the system is defined.	
		IAC-25_A05	circumstances requiring users to log out of the system are defined.	
YES		IAC-15_A48	system account types allowed are defined.	
YES		IAC-15.7_A01	system account types allowed are defined.	
YES		IAC-15_A49	system account types prohibited are defined.	
YES		IAC-15.7_A02	system account types prohibited are defined.	
YES	E-HRS-12 E-HRS-18 E-HRS-19	IAC-07_A03	system accounts are created in accordance with organizational policy, procedures, prerequisites, and criteria.	
YES		IAC-15.7_A04	system accounts are created in accordance with organizational policy, procedures, prerequisites, and criteria.	
YES	E-HRS-12 E-HRS-18 E-HRS-19	IAC-07_A04	system accounts are enabled in accordance with organizational policy, procedures, prerequisites, and criteria.	
YES		IAC-15.7_A05	system accounts are enabled in accordance with organizational policy, procedures, prerequisites, and criteria.	
YES	E-HRS-12 E-HRS-18 E-HRS-19	IAC-07_A05	system accounts are modified in accordance with organizational policy, procedures, prerequisites, and criteria.	
YES		IAC-15.7_A06	system accounts are modified in accordance with organizational policy, procedures, prerequisites, and criteria.	
YES	E-HRS-12 E-HRS-18 E-HRS-19	IAC-07_A06	system accounts are disabled in accordance with organizational policy, procedures, prerequisites, and criteria.	
YES		IAC-15.7_A07	system accounts are disabled in accordance with organizational policy, procedures, prerequisites, and criteria.	
YES	E-HRS-12 E-HRS-18 E-HRS-19	IAC-07_A07	system accounts are removed in accordance with organizational policy, procedures, prerequisites, and criteria.	
YES		IAC-15.7_A08	system accounts are removed in accordance with organizational policy, procedures, prerequisites, and criteria.	
YES		IAC-15_A41	authorized users of the system are specified.	
YES		IAC-15.7_A09	authorized users of the system are specified.	
	E-HRS-12 E-IAM-02	IAC-07.2_A16	group and role memberships are specified.	
	E-HRS-12 E-IAM-02	IAC-07.2_A17	access authorizations (i.e., privileges) for each account are specified.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
		IAC-01.2_A01	access to the system is authorized based on a valid access authorization.	
		IAC-01.2_A07	access to the system is authorized based on intended system usage.	
YES		IAC-15_A18	the use of system accounts is monitored.	
YES		IAC-15_A19	system accounts are disabled when the accounts have expired.	
YES		IAC-15_A20	system accounts are disabled when the accounts have been inactive for <A.03.01.01.ODP[01]: time period>.	US DoD ODP Value: at most 90 days
YES		IAC-15.3_A06	system accounts are disabled when the accounts have been inactive for <A.03.01.01.ODP[01]: time period>.	US DoD ODP Value: at most 90 days
YES		IAC-15_A21	system accounts are disabled when the accounts are no longer associated with a user or individual.	
YES		IAC-15_A22	system accounts are disabled when the accounts violate organizational policy.	
YES		IAC-15_A23	system accounts are disabled when significant risks associated with individuals are discovered.	
YES		IAC-15_A50	account managers and designated personnel or roles are notified within <A.03.01.01.ODP[02]: time period> when accounts are no longer required.	US DoD ODP Value: 24 hours
YES		IAC-15_A51	account managers and designated personnel or roles are notified within <A.03.01.01.ODP[03]: time period> when users are terminated or transferred.	US DoD ODP Value: 24 hours
YES		IAC-15_A52	account managers and designated personnel or roles are notified within <A.03.01.01.ODP[04]: time period> when system usage or the need-to-know changes for an individual.	US DoD ODP Value: 24 hours
		IAC-25_A06	users are required to log out of the system after <A.03.01.01.ODP[05]: time period> of expected inactivity or when the following circumstances occur: <A.03.01.01.ODP[06]: circumstances>.	US DoD ODP Values: [05] - at most 24 hours [06] - the work period ends, for privileged users at a minimum
N/A	N/A	N/A	N/A	N/A
	E-DCH-08	CFG-08_A03	approved authorizations for logical access to CUI are enforced in accordance with applicable access control policies.	
YES	E-IAM-02 E-IAM-05 E-IAM-06	IAC-21_A05	approved authorizations for logical access to system resources are enforced in accordance with applicable access control policies.	
N/A	N/A	N/A	N/A	N/A
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A09	approved authorizations are enforced for controlling the flow of CUI within the system.	
YES	E-AST-01 E-AST-27	END-01_A10	approved authorizations are enforced for controlling the flow of CUI within the system.	
YES	E-AST-12 E-AST-19	NET-04_A06	approved authorizations are enforced for controlling the flow of CUI between connected systems.	
		NET-05_A16	approved authorizations are enforced for controlling the flow of CUI between connected systems.	
N/A	N/A	N/A	N/A	N/A
	E-HRS-25	HRS-11_A04	duties of individuals requiring separation are identified.	
N/A	N/A	N/A	N/A	N/A

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
	E-HRS-12 E-IAM-02	IAC-08_A09	security functions for authorized access are defined.	
	E-HRS-12 E-IAM-02	IAC-08_A10	security-relevant information for authorized access is defined.	
YES	E-HRS-12 E-HRS-14 E-IAM-01	IAC-17_A01	the frequency at which to review the privileges assigned to roles or classes of users is defined.	
YES	E-IAM-02 E-IAM-05 E-IAM-06	IAC-21_A06	system access for users (or processes acting on behalf of users) is authorized only when necessary to accomplish assigned organizational tasks.	
	E-HRS-12 E-IAM-02	IAC-08_A11	access to <A.03.01.05.ODP[01]: security functions> is authorized.	US DoD ODP Value: 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
YES		IAC-20.1_A02	access to <A.03.01.05.ODP[01]: security functions> is authorized.	US DoD ODP Value: 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
	E-HRS-12 E-IAM-02	IAC-08_A12	access to <A.03.01.05.ODP[02]: security-relevant information> is authorized.	US DoD ODP Value: 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
YES		IAC-20.1_A03	access to <A.03.01.05.ODP[02]: security-relevant information> is authorized.	US DoD ODP Value: 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
YES	E-HRS-12 E-HRS-14 E-IAM-01	IAC-17_A03	the privileges assigned to roles or classes of users are reviewed <A.03.01.05.ODP[03]: frequency> to validate the need for such privileges.	US DoD ODP Value: at least every 12 months
YES	E-HRS-12 E-HRS-14 E-IAM-01	IAC-17_A04	privileges are reassigned or removed, as necessary.	
N/A	N/A	N/A	N/A	N/A
YES		IAC-21.3_A01	personnel or roles to which privileged accounts on the system are to be restricted are defined.	
YES		IAC-21.3_A02	privileged accounts on the system are restricted to <A.03.01.06.ODP[01]: personnel or roles>.	US DoD ODP Value: only defined and authorized personnel or administrative roles
		IAC-21.2_A02	users (or roles) with privileged accounts are required to use non-privileged accounts when accessing non-security functions or non-security information.	
N/A	N/A	N/A	N/A	N/A
		IAC-21.5_A03	non-privileged users are prevented from executing privileged functions.	
		MON-03.3_A02	the execution of privileged functions is logged.	
N/A	N/A	N/A	N/A	N/A

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
		IAC-22_A03	the number of consecutive invalid logon attempts by a user allowed during a time period is defined.	
		IAC-22_A05	the time period to which the number of consecutive invalid logon attempts by a user is limited is defined.	
		IAC-22_A10	one or more of the following PARAMETER VALUES are selected: {the account or node is locked automatically for <A.03.01.08.ODP[04]: time period>; the account or node is locked automatically until released by an administrator; the next logon prompt is delayed automatically; the system administrator is notified automatically; other action is taken automatically}.	US DoD ODP Value: at least 15- minute time period
		IAC-22_A06	the time period for an account or node to be locked is defined (if selected).	
		IAC-22_A09	a limit of <A.03.01.08.ODP[01]: number> consecutive invalid logon attempts by a user during <A.03.01.08.ODP[02]: time period> is enforced.	US DoD ODP Values: [01] - at most five (5) [02] - period of five (5) minutes
		IAC-22_A04	<A.03.01.08.ODP[03]: SELECTED PARAMETER VALUES> when the maximum number of unsuccessful attempts is exceeded.	US DoD 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
N/A	N/A	N/A	N/A	N/A
		SEA-18_A12	a system use notification message with privacy and security notices consistent with applicable CUI rules is displayed before granting access to the system.	
		SEA-18.1_A02	a system use notification message with privacy and security notices consistent with applicable CUI rules is displayed before granting access to the system.	
		SEA-18.2_A02	a system use notification message with privacy and security notices consistent with applicable CUI rules is displayed before granting access to the system.	
N/A	N/A	N/A	N/A	N/A
		IAC-24_A09	one or more of the following PARAMETER VALUES are selected: {a device lock is initiated after <A.03.01.10.ODP[02]: time period> of inactivity; the user is required to initiate a device lock before leaving the system unattended}.	US DoD ODP Value: at most 15- minute time period
		IAC-24_A06	the time period of inactivity after which a device lock is initiated is defined (if selected).	
		IAC-24_A07	access to the system is prevented by <A.03.01.10.ODP[01]: SELECTED PARAMETER VALUES>.	US DoD 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
		IAC-24_A08	the device lock is retained until the user reestablishes access using established identification and authentication procedures.	
		IAC-24.1_A01	information previously visible on the display is concealed via device lock with a publicly viewable image.	
N/A	N/A	N/A	N/A	N/A
		IAC-25_A02	conditions or trigger events that require session disconnect are defined.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
		IAC-25_A08	a user session is terminated automatically after <A.03.01.11.ODP[01]: conditions or trigger events>.	US DoD 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)
N/A	N/A	N/A	N/A	N/A
YES	E-NET-03	NET-14_A02	types of allowable remote system access are defined.	
YES	E-NET-03	NET-14_A01	usage restrictions are established for each type of allowable remote system access.	
YES	E-NET-03	NET-14_A05	configuration requirements are established for each type of allowable remote system access.	
YES	E-NET-03	NET-14_A03	connection requirements are established for each type of allowable remote system access.	
YES	E-NET-03	NET-14_A04	each type of remote system access is authorized prior to establishing such connections.	
YES	E-NET-03	NET-14_A09	remote access to the system is routed through authorized access control points.	
YES	E-NET-03	NET-14_A10	remote access to the system is routed through managed access control points.	
YES	E-NET-03	NET-14_A11	remote execution of privileged commands is authorized.	
		NET-14.4_A06	remote execution of privileged commands is authorized.	
YES	E-NET-03	NET-14_A12	remote access to security-relevant information is authorized.	
		NET-14.4_A07	remote access to security-relevant information is authorized.	
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
		NET-02.2_A03	each type of wireless access to the system is defined.	
		NET-15_A05	each type of wireless access to the system is defined.	
		NET-02.2_A04	usage restrictions are established for each type of wireless access to the system.	
		NET-15_A01	usage restrictions are established for each type of wireless access to the system.	
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A10	configuration requirements are established for each type of wireless access to the system.	
		NET-02.2_A05	connection requirements are established for each type of wireless access to the system.	
		NET-15_A02	connection requirements are established for each type of wireless access to the system.	
	E-IAM-06	IAC-01.2_A08	each type of wireless access to the system is authorized prior to establishing such connections.	
		NET-02.2_A06	each type of wireless access to the system is authorized prior to establishing such connections.	
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A11	wireless networking capabilities not intended for use are disabled prior to issuance and deployment.	
		NET-15.1_A01	wireless access to the system is protected using authentication.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
		NET-15.1_A02	wireless access to the system is protected using encryption.	
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
YES		MDM-01_A02	usage restrictions are established for mobile devices.	
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A12	configuration requirements are established for mobile devices.	
YES		NET-03_A21	connection requirements are established for mobile devices.	
		MDM-02_A04	the connection of mobile devices to the system is authorized.	
		MDM-03_A05	full-device or container-based encryption is implemented to protect the confidentiality of CUI on mobile devices.	
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
		DCH-13_A13	security requirements to be satisfied on external systems prior to allowing the use of or access to those systems by authorized individuals are defined.	
		DCH-13_A14	the use of external systems is prohibited unless the systems are specifically authorized.	
		DCH-13_A15	the following security requirements to be satisfied on external systems prior to allowing the use of or access to those systems by authorized individuals are established: <A.03.01.20.ODP[01]: security requirements>.	US DoD 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.
		DCH-13_A16	authorized individuals are permitted to use external systems to access the organizational system or to process, store, or transmit CUI only after verifying that the security requirements on the external systems as specified in the organization’s system security plans have been satisfied.	
		DCH-13_A17	authorized individuals are permitted to use external systems to access the organizational system or to process, store, or transmit CUI only after retaining approved system connection or processing agreements with the organizational entity hosting the external systems.	
		DCH-13.2_A05	the use of organization-controlled portable storage devices by authorized individuals on external systems is restricted.	
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
YES		DCH-15_A08	authorized individuals are trained to ensure that publicly accessible information does not contain CUI.	
YES		DCH-15_A11	the content on publicly accessible systems is reviewed for CUI.	
YES		DCH-15_A09	CUI is removed from publicly accessible systems, if discovered.	
		IRO-12_A09	CUI is removed from publicly accessible systems, if discovered.	
N/A	N/A	N/A	N/A	N/A
	E-SAT-02 E-SAT-04 E-SAT-05	SAT-01_A03	the frequency at which to provide security literacy training to system users after initial training is defined.	
	E-SAT-02 E-SAT-04 E-SAT-05	SAT-01_A04	events that require security literacy training for system users are defined.	
	E-SAT-02	SAT-02_A11	the frequency at which to update security literacy training content is defined.	
	E-SAT-02	SAT-02_A12	events that require security literacy training content updates are defined.	
	E-SAT-02 E-SAT-04 E-SAT-05	SAT-01_A05	security literacy training is provided to system users as part of initial training for new users.	
	E-SAT-02 E-SAT-04 E-SAT-05	SAT-01_A06	security literacy training is provided to system users <A.03.02.01.ODP[01]: frequency> after initial training.	US DoD ODP Value: at least every 12 months
	E-SAT-04	SAT-03.6_A05	security literacy training is provided to system users when required by system changes or following <A.03.02.01.ODP[02]: events>.	US DoD ODP Value: significant, novel incidents, or significant changes to risks
	E-SAT-04 E-SAT-05 E-THR-04	THR-05_A02	security literacy training is provided to system users on recognizing indicators of insider threat.	
	E-SAT-04 E-SAT-05 E-THR-04	THR-05_A03	security literacy training is provided to system users on reporting indicators of insider threat.	
	E-SAT-02	SAT-02.2_A02	security literacy training is provided to system users on recognizing indicators of social engineering.	
	E-SAT-02	SAT-02.2_A03	security literacy training is provided to system users on reporting indicators of social engineering.	
	E-SAT-02	SAT-02.2_A04	security literacy training is provided to system users on recognizing indicators of social mining.	
	E-SAT-02	SAT-02.2_A05	security literacy training is provided to system users on reporting indicators of social mining.	
	E-SAT-04	SAT-03.6_A06	security literacy training content is updated <A.03.02.01.ODP[03]: frequency>.	US DoD ODP Value: at least every 12 months
	E-SAT-04	SAT-03.6_A07	security literacy training content is updated following <A.03.02.01.ODP[04]: events>.	US DoD ODP Value: significant, novel incidents, or significant changes to risks
N/A	N/A	N/A	N/A	N/A
	E-SAT-05	SAT-03_A07	the frequency at which to provide role-based security training to assigned personnel after initial training is defined.	
	E-SAT-05	SAT-03_A12	events that require role-based security training are defined.	
	E-SAT-05	SAT-03_A08	the frequency at which to update role-based security training content is defined.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
	E-SAT-05	SAT-03_A02	events that require role-based security training content updates are defined.	
	E-SAT-05	SAT-03_A16	role-based security training is provided to organizational personnel before authorizing access to the system or CUI.	
	E-SAT-05	SAT-03_A04	role-based security training is provided to organizational personnel before performing assigned duties.	
	E-SAT-05	SAT-03_A17	role-based security training is provided to organizational personnel <A.03.02.02.ODP[01]: frequency> after initial training.	US DoD ODP Value: at least every 12 months
	E-SAT-05	SAT-03_A18	role-based security training is provided to organizational personnel when required by system changes or following <A.03.02.02.ODP[02]: events>.	US DoD ODP Value: significant, novel incidents, or significant changes to risks
	E-SAT-05		role-based security training content is updated <A.03.02.02.ODP[03]: frequency>.	US DoD ODP Value: at least every 12 months
	E-SAT-05		role-based security training content is updated following <A.03.02.02.ODP[04]: events>.	US DoD ODP Value: significant, novel incidents, or significant changes to risks
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
YES	E-AST-01 E-CPL-01	MON-03_A12	event types selected for logging within the system are defined.	
YES	E-MON-01 E-MON-02 E-MON-05	MON-01.8_A06	the frequency of event types selected for logging are reviewed and updated.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
YES	E-AST-01 E-CPL-01	MON-03_A13	the following event types are specified for logging within the system: <A.03.03.01.ODP[01]: event types>.	applicable: (1) Authentication events: (a) Logons (Success/Failure) (b) Logoffs (Success) (2) Security Relevant File and Objects events: (a) Create (Success/Failure) (b) Access (Success/Failure) (c) Delete (Success/Failure) (d) Modify (Success/Failure) (e) Permission Modification (Success/Failure) (f) Ownership Modification (Success/Failure) (3) Export/Writes/downloads to devices/digital media (e.g., CD/DVD, USB, SD) (Success/Failure) (4) Import/Uploads from devices/digital media (e.g., CD/DVD, USB, SD) (Success/Failure) (5) User and Group Management events: (a) User add, delete, modify, disable, lock (Success/Failure) (b) Group/Role add, delete, modify (Success/Failure) 6) Use of Privileged/Special Rights events: (a) Security or audit policy changes (Success/Failure) (b) Configuration changes (Success/Failure) (7) Admin or root-level access (Success/Failure) (8) Privilege/Role escalation (Success/Failure) (9) Audit and security relevant log data accesses (Success/Failure) (10) System reboot, restart, and shutdown (Success/Failure) (11) Print to a device (Success/Failure) (12) Print to a file (e.g., pdf format) (Success/Failure) (13) Application (e.g., Adobe, Firefox, MS Office Suite) initialization (Success/Failure)
YES	E-MON-01 E-MON-02 E-MON-05	MON-01.8_A09	the event types selected for logging are reviewed <A.03.03.01.ODP[02]: frequency>.	US DoD ODP Value: at least every 12 months and after any significant incidents or significant changes to risks
YES	E-AST-01 E-CPL-01	MON-03_A14	the event types selected for logging are updated <A.03.03.01.ODP[02]: frequency>.	US DoD ODP Value: at least every 12 months and after any significant incidents or significant changes to risks
N/A	N/A	N/A	N/A	N/A
	E-MON-01 E-MON-06 E-MON-07	MON-01.4_A01	audit records contain information that establishes what type of event occurred.	
YES	E-AST-01 E-CPL-01	MON-03_A03	audit records contain information that establishes when the event occurred.	
YES	E-AST-01 E-CPL-01	MON-03_A04	audit records contain information that establishes where the event occurred.	
YES	E-AST-01 E-CPL-01	MON-03_A05	audit records contain information that establishes the source of the event.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
YES	E-AST-01 E-CPL-01	MON-03_A06	audit records contain information that establishes the outcome of the event.	
YES	E-AST-01 E-CPL-01	MON-03_A07	audit records contain information that establishes the identity of the individuals, subjects, objects, or entities associated with the event.	
YES	E-AST-01 E-CPL-01	MON-03_A15	additional information for audit records is provided, as needed.	
		CFG-02.9_A02	additional information for audit records is provided, as needed.	
N/A	N/A	N/A	N/A	N/A
	E-MON-01 E-MON-06 E-MON-07	MON-01.4_A06	audit records for the selected event types and audit record content specified in 03.03.01 and 03.03.02 are generated.	
YES		MON-08_A01	audit records are retained for a time period consistent with the records retention policy.	
YES	E-AST-11	MON-10_A02	audit records are retained for a time period consistent with the records retention policy.	
N/A	N/A	N/A	N/A	N/A
		MON-05_A05	the time period for organizational personnel or roles receiving audit logging process failure alerts is defined.	
		MON-05_A06	additional actions to be taken in the event of an audit logging process failure are defined.	
		MON-05_A07	organizational personnel or roles are alerted in the event of an audit logging process failure within <A.03.03.04.ODP[01]: time period>.	US DoD ODP Value: near real time or as soon as practicable upon discovery
		MON-05_A08	the following additional actions are taken: <A.03.03.04.ODP[02]: additional actions>.	US DoD ODP Value: document the failure and resolution, troubleshoot, repair/restart the audit logging process, and report as incident if applicable
N/A	N/A	N/A	N/A	N/A
YES	E-MON-01 E-MON-02 E-MON-05	MON-01.8_A01	the frequency at which system audit records are reviewed and analyzed is defined.	
YES	E-MON-01 E-MON-05	MON-02_A01	the frequency at which system audit records are reviewed and analyzed is defined.	
YES	E-MON-01 E-MON-02 E-MON-05	MON-01.8_A10	system audit records are reviewed and analyzed <A.03.03.05.ODP[01]: frequency> for indications and the potential impact of inappropriate or unusual activity.	US DoD ODP Value: at least weekly
YES	E-MON-01 E-MON-05	MON-02_A13	system audit records are reviewed and analyzed <A.03.03.05.ODP[01]: frequency> for indications and the potential impact of inappropriate or unusual activity.	US DoD ODP Value: at least weekly

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
	E-MON-06	MON-01.12_A05	findings are reported to organizational personnel or roles.	
		MON-06_A06	findings are reported to organizational personnel or roles.	
YES	E-MON-01 E-MON-05	MON-02_A03	audit records across different repositories are analyzed to gain organization-wide situational awareness.	
	E-MON-05 E-MON-07	MON-02.1_A04	audit records across different repositories are correlated to gain organization-wide situational awareness.	
N/A	N/A	N/A	N/A	N/A
		MON-06_A07	an audit record reduction and report generation capability that supports audit record review is implemented.	
		MON-06_A08	an audit record reduction and report generation capability that supports audit record analysis is implemented.	
		MON-06_A09	an audit record reduction and report generation capability that supports audit record reporting requirements is implemented.	
		MON-06_A10	an audit record reduction and report generation capability that supports after-the-fact investigations of incidents is implemented.	
YES		MON-08_A02	the original content of audit records is preserved.	
YES		MON-08_A03	the original time ordering of audit records is preserved.	
N/A	N/A	N/A	N/A	N/A
YES		MON-07_A03	granularity of time measurement for audit record time stamps is defined.	
YES		MON-07_A02	internal system clocks are used to generate time stamps for audit records.	
YES		MON-07_A05	time stamps are recorded for audit records that meet <A.03.03.07.ODP[01]: granularity of time measurement>.	US DoD ODP Value: a granularity of one (1) second or smaller
		MON-07.1_A06	time stamps are recorded for audit records 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.	
N/A	N/A	N/A	N/A	N/A
YES		MON-08_A04	audit information is protected from unauthorized access, modification, and deletion.	
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A13	audit logging tools are protected from unauthorized access, modification, and deletion.	
YES		MON-08_A05	access to management of audit logging functionality is authorized to only a subset of privileged users or roles.	
		MON-08.2_A02	access to management of audit logging functionality is authorized to only a subset of privileged users or roles.	
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
	E-AST-12	CFG-02.1_A03	the frequency of baseline configuration review and update is defined.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A14	a current baseline configuration of the system is developed.	
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A15	a current baseline configuration of the system is maintained under configuration control.	
	E-AST-12	CFG-02.1_A09	the baseline configuration of the system is reviewed <A.03.04.01.ODP[01]: frequency>.	US DoD ODP Value: at least every 12 months and after any significant incidents or significant changes occur
	E-AST-12	CFG-02.1_A10	the baseline configuration of the system is updated <A.03.04.01.ODP[01]: frequency>.	US DoD ODP Value: at least every 12 months and after any significant incidents or significant changes occur
	E-AST-12	CFG-02.1_A06	the baseline configuration of the system is reviewed when system components are installed or modified.	
	E-AST-12	CFG-02.1_A07	the baseline configuration of the system is updated when system components are installed or modified.	
N/A	N/A	N/A	N/A	N/A
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-03_A13	configuration settings for the system that reflect the most restrictive mode consistent with operational requirements are defined.	
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A16	the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements are established and documented: <A.03.04.02.ODP[01]: configuration settings>.	US DoD 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 (https://ncp.nist.gov/repository) 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.
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A17	the following configuration settings for the system are implemented: <A.03.04.02.ODP[01]: configuration settings>.	US DoD 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 (https://ncp.nist.gov/repository) 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.

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
		CFG-02.7_A03	any deviations from established configuration settings are identified and documented.	
		CFG-02.7_A04	any deviations from established configuration settings are approved.	
N/A	N/A	N/A	N/A	N/A
	E-AST-01	CFG-01_A02	the types of changes to the system that are configuration-controlled are defined.	
	E-CHG-02	CHG-02_A06	the types of changes to the system that are configuration-controlled are defined.	
	E-CHG-04	CHG-03_A01	proposed configuration-controlled changes to the system are reviewed with explicit consideration for security impacts.	
YES	E-CHG-02	CHG-02.1_A11	proposed configuration-controlled changes to the system are approved or disapproved with explicit consideration for security impacts.	
	E-CHG-02	CHG-02_A03	approved configuration-controlled changes to the system are implemented.	
YES	E-MNT-04	MNT-02_A02	approved configuration-controlled changes to the system are implemented.	
	E-CHG-03	CHG-02.2_A09	approved configuration-controlled changes to the system are documented.	
		CFG-02.2_A05	activities associated with configuration-controlled changes to the system are monitored.	
YES	E-CHG-02	CHG-01_A12	activities associated with configuration-controlled changes to the system are monitored.	
		CFG-02.2_A06	activities associated with configuration-controlled changes to the system are reviewed.	
YES	E-CHG-02	CHG-01_A13	activities associated with configuration-controlled changes to the system are reviewed.	
N/A	N/A	N/A	N/A	N/A
	E-CHG-04	CHG-03_A02	changes to the system are analyzed to determine potential security impacts prior to change implementation.	
		CHG-06_A03	the security requirements for the system continue to be satisfied after the system changes have been implemented.	
N/A	N/A	N/A	N/A	N/A
	E-PES-03 E-PES-05	PES-02.1_A02	physical access restrictions associated with changes to the system are defined and documented.	
	E-PES-03 E-PES-05	PES-02_A11	physical access restrictions associated with changes to the system are approved.	
YES	E-PES-05	PES-03_A25	physical access restrictions associated with changes to the system are enforced.	
	E-HRS-12 E-IAM-02	IAC-08_A13	logical access restrictions associated with changes to the system are defined and documented.	
YES	E-CHG-02	CHG-02.1_A12	logical access restrictions associated with changes to the system are approved.	
		CHG-04.4_A02	logical access restrictions associated with changes to the system are enforced.	
N/A	N/A	N/A	N/A	N/A
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A18	functions to be prohibited or restricted are defined.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A19	ports to be prohibited or restricted are defined.	
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A20	protocols to be prohibited or restricted are defined.	
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A21	connections to be prohibited or restricted are defined.	
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A22	services to be prohibited or restricted are defined.	
		CFG-03.1_A01	the frequency at which to review the system to identify unnecessary or nonsecure functions, ports, protocols, connections, or services is defined.	
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A23	the use of the following functions is prohibited or restricted: <A.03.04.06.ODP[01]: functions>.	US DoD 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.
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A24	the use of the following ports is prohibited or restricted: <A.03.04.06.ODP[02]: ports>.	US DoD 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.

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A25	the use of the following protocols is prohibited or restricted: <A.03.04.06.ODP[03]: protocols>.	US DoD 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.
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A26	the use of the following connections is prohibited or restricted: <A.03.04.06.ODP[04]: connections>.	US DoD 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.
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A27	the use of the following services is prohibited or restricted: <A.03.04.06.ODP[05]: services>.	US DoD 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.
	E-AST-12	CFG-02.1_A08	the system is reviewed <A.03.04.06.ODP[06]: frequency> to identify unnecessary or nonsecure functions, ports, protocols, connections, and services.	US DoD ODP Value: at least every 12 months, when any system functions, ports, protocols, or services changes are made, and after any significant incidents or significant changes to risks
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-03_A14	unnecessary or nonsecure functions, ports, protocols, connections, and services are disabled or removed.	
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
		CFG-03.3_A12	the frequency at which to review and update the list of authorized software programs is defined.	
		CFG-03.3_A11	software programs authorized to execute on the system are identified.	
		CFG-03.3_A13	a deny-all, allow-by-exception policy for the execution of authorized software programs on the system is implemented.	
		AST-01.4_A02	the list of authorized software programs is reviewed and updated <A.03.04.08.ODP[01]: frequency>.	US DoD ODP Value: at least quarterly
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
YES	E-AST-04 E-AST-05 E-AST-07	AST-02_A08	the frequency at which to review and update the system component inventory is defined.	
YES	E-AST-04 E-AST-05 E-AST-07	AST-02_A09	an inventory of system components is developed and documented.	
YES	E-AST-04 E-AST-05 E-AST-07	AST-02_A10	the system component inventory is reviewed <A.03.04.10.ODP[01]: frequency>.	US DoD ODP Value: at least quarterly
YES	E-AST-04 E-AST-05 E-AST-07	AST-02_A11	the system component inventory is updated <A.03.04.10.ODP[01]: frequency>.	US DoD ODP Value: at least quarterly
		AST-02.1_A01	the system component inventory is updated as part of component installations.	
		AST-02.1_A02	the system component inventory is updated as part of component removals.	
		AST-02.1_A03	the system component inventory is updated as part of system updates.	
N/A	N/A	N/A	N/A	N/A
	E-DCH-05	AST-02.8_A07	the location of CUI is identified and documented.	
YES	E-AST-23	DCH-24_A09	the location of CUI is identified and documented.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
	E-DCH-05	AST-02.8_A08	the system components on which CUI is processed are identified and documented.	
	E-TDA-14	IAO-03_A59	the system components on which CUI is processed are identified and documented.	
	E-DCH-05	AST-02.8_A09	the system components on which CUI is stored are identified and documented.	
	E-TDA-14	IAO-03_A60	the system components on which CUI is stored are identified and documented.	
	E-DCH-05	AST-02.8_A10	changes to the system or system component location where CUI is processed are documented.	
		CHG-05_A04	changes to the system or system component location where CUI is processed are documented.	
	E-TDA-14	IAO-03_A61	changes to the system or system component location where CUI is processed are documented.	
	E-DCH-05	AST-02.8_A11	changes to the system or system component location where CUI is stored are documented.	
		CHG-05_A05	changes to the system or system component location where CUI is stored are documented.	
	E-TDA-14	IAO-03_A62	changes to the system or system component location where CUI is stored are documented.	
N/A	N/A	N/A	N/A	N/A
	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02.5_A04	configurations for systems or system components to be issued to individuals traveling to high-risk locations are defined.	
	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02.5_A01	security requirements to be applied to the system or system components when individuals return from travel are defined.	
		AST-24_A04	systems or system components with the following configurations are issued to individuals traveling to high-risk locations: <A.03.04.12.ODP[01]: configurations>.	US DoD 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
		AST-25_A03	the following security requirements are applied to the system or system components when the individuals return from travel: <A.03.04.12.ODP[02]: security requirements>.	US DoD 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
N/A	N/A	N/A	N/A	N/A
		IAC-14_A01	circumstances or situations that require re-authentication are defined.	
	E-IAM-06	IAC-01.2_A02	system users are uniquely identified.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
	E-IAM-06	IAC-01.2_A03	system users are authenticated.	
	E-IAM-05 E-IAM-06	IAC-02_A03	processes acting on behalf of users are associated with uniquely identified and authenticated system users.	
		IAC-14_A03	users are reauthenticated when <A.03.05.01.ODP[01]: circumstances or situations>.	US DoD 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
N/A	N/A	N/A	N/A	N/A
	E-IAM-05 E-IAM-06	IAC-04_A01	devices or types of devices to be uniquely identified and authenticated before establishing a connection are defined.	
	E-IAM-05 E-IAM-06	IAC-04_A10	<A.03.05.02.ODP[01]: devices or types of devices> are uniquely identified before establishing a system connection.	US DoD ODP Value: all devices for identification, where feasible for authentication, and document when not feasible
	E-IAM-05 E-IAM-06	IAC-04_A11	<A.03.05.02.ODP[01]: devices or types of devices> are authenticated before establishing a system connection.	US DoD ODP Value: all devices for identification, where feasible for authentication, and document when not feasible
N/A	N/A	N/A	N/A	N/A
		IAC-06_A01	multi-factor authentication for access to privileged accounts is implemented.	
		IAC-06.4_A01	multi-factor authentication for access to privileged accounts is implemented.	
		IAC-06_A02	multi-factor authentication for access to non-privileged accounts is implemented.	
		IAC-06.4_A02	multi-factor authentication for access to non-privileged accounts is implemented.	
N/A	N/A	N/A	N/A	N/A
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A28	replay-resistant authentication mechanisms for access to privileged accounts are implemented.	
	E-AST-01 E-IAM-05 E-IAM-06	IAC-02.2_A01	replay-resistant authentication mechanisms for access to privileged accounts are implemented.	
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A29	replay-resistant authentication mechanisms for access to non-privileged accounts are implemented.	
	E-AST-01 E-IAM-05 E-IAM-06	IAC-02.2_A02	replay-resistant authentication mechanisms for access to non-privileged accounts are implemented.	
N/A	N/A	N/A	N/A	N/A
		IAC-09_A03	the time period for preventing the reuse of identifiers is defined.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
		IAC-09.2_A01	characteristic used to identify individual status are defined.	
YES	E-HRS-12 E-HRS-18 E-HRS-19	IAC-07_A02	authorization is received from organizational personnel or roles to assign an individual, group, role, service, or device identifier.	
		IAC-09_A05	an identifier that identifies an individual, group, role, service, or device is selected.	
		IAC-09_A06	an identifier that identifies an individual, group, role, service, or device is assigned.	
		IAC-09_A07	the reuse of identifiers for <A.03.05.05.ODP[01]: time period> is prevented.	US DoD ODP Value: at least ten (10) years
	E-IAM-05 E-IAM-06	IAC-02_A08	individual identifiers are managed by uniquely identifying each individual as <A.03.05.05.ODP[02]: characteristic>.	US DoD ODP Value: privileged or non-privileged users; contractors, foreign nationals, and/or non-organizational users
		IAC-09.2_A03	individual identifiers are managed by uniquely identifying each individual as <A.03.05.05.ODP[02]: characteristic>.	US DoD ODP Value: privileged or non-privileged users; contractors, foreign nationals, and/or non-organizational users
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
		IAC-10.4_A05	the frequency at which to update the list of commonly used, expected, or compromised passwords is defined.	
		IAC-10.11_A08	the frequency at which to update the list of commonly used, expected, or compromised passwords is defined.	
		IAC-10.1_A09	password composition and complexity rules are defined.	
		IAC-10.4_A06	a list of commonly used, expected, or compromised passwords is maintained.	
		IAC-10.11_A09	a list of commonly used, expected, or compromised passwords is maintained.	
		IAC-10.4_A10	a list of commonly used, expected, or compromised passwords is updated <A.03.05.07.ODP[01]: frequency>.	US DoD ODP Value: at least quarterly
		IAC-10.11_A13	a list of commonly used, expected, or compromised passwords is updated <A.03.05.07.ODP[01]: frequency>.	US DoD ODP Value: at least quarterly
		IAC-10.4_A08	a list of commonly used, expected, or compromised passwords is updated when organizational passwords are suspected to have been compromised.	
		IAC-10.11_A11	a list of commonly used, expected, or compromised passwords is updated when organizational passwords are suspected to have been compromised.	
		IAC-10.4_A09	passwords are verified not to be found on the list of commonly used, expected, or compromised passwords when they are created or updated by users.	
		IAC-10.11_A12	passwords are verified not to be found on the list of commonly used, expected, or compromised passwords when they are created or updated by users.	
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A30	passwords are only transmitted over cryptographically protected channels.	
YES		IAC-10.5_A06	passwords are only transmitted over cryptographically protected channels.	
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A31	passwords are stored in a cryptographically protected form.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
YES		IAC-10.5_A04	passwords are stored in a cryptographically protected form.	
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A32	a new password is selected upon first use after account recovery.	
YES		IAC-15_A53	a new password is selected upon first use after account recovery.	
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A35	the following composition and complexity rules for passwords are enforced: <A.03.05.07.ODP[02]: rules>.	US DoD ODP Values: (1) Must have a minimum length of 16 characters. (2) Contains a string of characters that does not include the user's account name or full name.
		IAC-10.1_A13	the following composition and complexity rules for passwords are enforced: <A.03.05.07.ODP[02]: rules>.	US DoD ODP Values: (1) Must have a minimum length of 16 characters. (2) Contains a string of characters that does not include the user's account name or full name.
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
		IAC-11_A02	feedback of authentication information during the authentication process is obscured.	
N/A	N/A	N/A	N/A	N/A
YES		IAC-10_A04	the frequency for changing or refreshing authenticators is defined.	
YES		IAC-10_A05	events that trigger the change or refreshment of authenticators are defined.	
YES		IAC-10_A06	the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution is verified.	
YES		IAC-10_A07	initial authenticator content for any authenticators issued by the organization is established.	
YES		IAC-10_A18	administrative procedures for initial authenticator distribution are established.	
YES		IAC-10_A19	administrative procedures for lost, compromised, or damaged authenticators are established.	
YES		IAC-10_A20	administrative procedures for revoking authenticators are established.	
YES		IAC-10_A21	administrative procedures for initial authenticator distribution are implemented.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
YES		IAC-10_A22	administrative procedures for lost, compromised, or damaged authenticators are implemented.	
YES		IAC-10_A23	administrative procedures for revoking authenticators are implemented.	
YES		IAC-10_A10	default authenticators are changed at first use.	
YES		IAC-10_A25	authenticators are changed or refreshed <A.03.05.12.ODP[01]: frequency> or when the following events occur: <A.03.05.12.ODP[02]: events>.	US DoD ODP Values: (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. (2) after a relevant security incident or any evidence of compromise or loss.
YES		IAC-10_A26	authenticator content is protected from unauthorized disclosure.	
YES		IAC-10.5_A02	authenticator content is protected from unauthorized disclosure.	
YES		IAC-10_A27	authenticator content is protected from unauthorized modification.	
YES		IAC-10.5_A03	authenticator content is protected from unauthorized modification.	
N/A	N/A	N/A	N/A	N/A
	E-IRO-01	IRO-01_A14	an incident-handling capability that is consistent with the incident response plan is implemented.	
YES	E-IRO-03	IRO-02_A02	the incident handling capability includes preparation.	
YES	E-IRO-03	IRO-02_A03	the incident handling capability includes detection and analysis.	
YES	E-IRO-03	IRO-02_A04	the incident handling capability includes containment.	
YES	E-IRO-03	IRO-02_A05	the incident handling capability includes eradication.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
YES	E-IRO-03	IRO-02_A06	the incident handling capability includes recovery.	
N/A	N/A	N/A	N/A	N/A
	E-IRO-01	IRO-04_A25	the time period to report suspected incidents to the organizational incident response capability is defined.	
	E-IRO-01 E-IRO-11	IRO-10_A01	the time period to report suspected incidents to the organizational incident response capability is defined.	
	E-IRO-01	IRO-04_A26	authorities to whom incident information is to be reported are defined.	
	E-IRO-01 E-IRO-11	IRO-10.2_A02	authorities to whom incident information is to be reported are defined.	
		IRO-14_A02	authorities to whom incident information is to be reported are defined.	
		IRO-09_A04	system security incidents are tracked.	
		IRO-09_A03	system security incidents are documented.	
YES	E-IRO-03	IRO-02_A22	suspected incidents are reported to the organizational incident response capability within <A.03.06.02.ODP[01]: time period>.	US DoD ODP Value: near real time or as soon as practicable upon discovery
	E-IRO-01 E-IRO-09	IRO-07_A09	suspected incidents are reported to the organizational incident response capability within <A.03.06.02.ODP[01]: time period>.	US DoD ODP Value: near real time or as soon as practicable upon discovery
	E-IRO-01 E-IRO-11	IRO-10_A07	suspected incidents are reported to the organizational incident response capability within <A.03.06.02.ODP[01]: time period>.	US DoD ODP Value: near real time or as soon as practicable upon discovery
	E-IRO-01 E-IRO-11	IRO-10_A08	incident information is reported to <A.03.06.02.ODP[02]: authorities>.	US DoD ODP Value: all applicable personnel and entities as specified by the contract, and in accordance with any incident response plan notification procedures
	E-IRO-01 E-IRO-09	IRO-07_A05	an incident response support resource that offers advice and assistance to system users on handling and reporting incidents is provided.	
	E-IRO-01 E-IRO-11	IRO-10_A06	an incident response support resource that offers advice and assistance to system users on handling and reporting incidents is provided.	
		IRO-11_A01	an incident response support resource that offers advice and assistance to system users on handling and reporting incidents is provided.	
N/A	N/A	N/A	N/A	N/A
	E-IRO-04	IRO-06_A01	the frequency at which to test the effectiveness of the incident response capability for the system is defined.	
	E-IRO-04	IRO-06_A07	the effectiveness of the incident response capability is tested <A.03.06.03.ODP[01]: frequency>.	US DoD ODP Value: at least every 12 months
N/A	N/A	N/A	N/A	N/A
	E-IRO-05 E-IRO-06	IRO-05_A05	the time period within which incident response training is to be provided to system users is defined.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
	E-IRO-05 E-IRO-06	IRO-05_A06	the frequency at which to provide incident response training to users after initial training is defined.	
	E-IRO-05 E-IRO-06	IRO-05_A07	the frequency at which to review and update incident response training content is defined.	
	E-IRO-05 E-IRO-06	IRO-05_A02	events that initiate a review of the incident response training content are defined.	
	E-IRO-08	IRO-13_A04	events that initiate a review of the incident response training content are defined.	
	E-IRO-05 E-IRO-06	IRO-05_A14	incident response training for system users consistent with assigned roles and responsibilities is provided within <A.03.06.04.ODP[01]: time period> of assuming an incident response role or responsibility or acquiring system access.	US DoD ODP Value: ten (10) days for privileged users, thirty (30) days for all other roles
	E-SAT-05	SAT-03_A21	incident response training for system users consistent with assigned roles and responsibilities is provided within <A.03.06.04.ODP[01]: time period> of assuming an incident response role or responsibility or acquiring system access.	US DoD ODP Value: ten (10) days for privileged users, thirty (30) days for all other roles
	E-SAT-05	SAT-03_A14	incident response training for system users consistent with assigned roles and responsibilities is provided when required by system changes.	
	E-SAT-05	SAT-03_A22	incident response training for system users consistent with assigned roles and responsibilities is provided <A.03.06.04.ODP[02]: frequency> thereafter.	US DoD ODP Value: at least every 12 months
	E-IRO-05 E-IRO-06	IRO-05_A15	incident response training content is reviewed <A.03.06.04.ODP[03]: frequency>.	US DoD ODP Value: at least every 12 months
	E-IRO-05 E-IRO-06	IRO-05_A16	incident response training content is updated <A.03.06.04.ODP[03]: frequency>.	US DoD ODP Value: at least every 12 months
	E-IRO-05 E-IRO-06	IRO-05_A17	incident response training content is reviewed following <A.03.06.04.ODP[04]: events>.	US DoD ODP Values: (1) at least every 12 months (2) significant, novel incidents, or significant changes to risks
	E-IRO-05 E-IRO-06	IRO-05_A18	incident response training content is updated following <A.03.06.04.ODP[04]: events>.	US DoD ODP Values: (1) at least every 12 months (2) significant, novel incidents, or significant changes to risks
N/A	N/A	N/A	N/A	N/A
	E-IRO-01	IRO-04_A03	an incident response plan is developed that provides the organization with a roadmap for implementing its incident response capability.	
	E-IRO-01	IRO-04_A04	an incident response plan is developed that describes the structure and organization of the incident response capability.	
	E-IRO-01	IRO-04_A05	an incident response plan is developed that provides a high-level approach for how the incident response capability fits into the overall organization.	
	E-IRO-01	IRO-04_A07	an incident response plan is developed that defines reportable incidents.	
	E-IRO-01	IRO-04_A10	an incident response plan is developed that addresses the sharing of incident information.	
	E-IRO-01	IRO-04_A12	an incident response plan is developed that designates responsibilities to organizational entities, personnel, or roles.	
	E-IRO-01	IRO-04_A13	copies of the incident response plan are distributed to designated incident response personnel (identified by name or by role).	
	E-IRO-01	IRO-04_A18	copies of the incident response plan are distributed to organizational elements.	
	E-IRO-07	IRO-04.2_A06	the incident response plan is updated to address system and organizational changes or problems encountered during plan implementation, execution, or testing.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
YES	E-HRS-01 E-HRS-02 E-HRS-03 E-HRS-04 E-HRS-11 E-HRS-13 E-HRS-18 E-HRS-22	HRS-03_A02	the incident response plan is protected from unauthorized disclosure.	
	E-HRS-12 E-IAM-02	IAC-08_A14	the incident response plan is protected from unauthorized disclosure.	
YES		IAC-20.1_A04	the incident response plan is protected from unauthorized disclosure.	
	E-IRO-01	IRO-04_A23	the incident response plan is protected from unauthorized disclosure.	ADDED -----
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
		MNT-04_A07	the use of system maintenance tools is approved.	
		MNT-04_A08	the use of system maintenance tools is controlled.	
		MNT-04_A09	the use of system maintenance tools is monitored.	
		MNT-04.2_A01	media with diagnostic and test programs are checked for malicious code before the media are used in the system.	
		MNT-04.3_A06	the removal of system maintenance equipment containing CUI is prevented by verifying that there is no CUI on the equipment, sanitizing or destroying the equipment, or retaining the equipment within the facility.	
N/A	N/A	N/A	N/A	N/A
		MNT-05_A01	nonlocal maintenance and diagnostic activities are approved.	
		MNT-05_A02	nonlocal maintenance and diagnostic activities are monitored.	
		IAC-06_A06	multi-factor authentication is implemented in the establishment of nonlocal maintenance and diagnostic sessions.	
YES	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21	CFG-02_A34	replay resistance is implemented in the establishment of nonlocal maintenance and diagnostic sessions.	
	E-AST-01 E-IAM-05 E-IAM-06	IAC-02.2_A03	replay resistance is implemented in the establishment of nonlocal maintenance and diagnostic sessions.	
		MNT-05.3_A04	replay resistance is implemented in the establishment of nonlocal maintenance and diagnostic sessions.	
		IAC-25_A07	session connections are terminated when nonlocal maintenance is completed.	
		MNT-05.4_A01	session connections are terminated when nonlocal maintenance is completed.	
		NET-07_A04	network connections are terminated when nonlocal maintenance is completed.	
N/A	N/A	N/A	N/A	N/A
		MNT-06_A01	a process for maintenance personnel authorization is established.	
		MNT-06_A02	a list of authorized maintenance organizations or personnel is maintained.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
		MNT-06_A03	non-escorted personnel who perform maintenance on the system possess the required access authorizations.	
		MNT-06.1_A13	non-escorted personnel who perform maintenance on the system possess the required access authorizations.	
	E-MNT-01	MNT-06.2_A02	non-escorted personnel who perform maintenance on the system possess the required access authorizations.	
		MNT-06.1_A02	organizational personnel with required access authorizations are designated to supervise the maintenance activities of personnel who do not possess the required access authorizations.	
		MNT-06.1_A14	organizational personnel with required technical competence are designated to supervise the maintenance activities of personnel who do not possess the required access authorizations.	
N/A	N/A	N/A	N/A	N/A
	E-DCH-02	DCH-06_A10	system media that contain CUI are physically controlled.	
	E-DCH-02	DCH-06_A11	system media that contain CUI are securely stored.	
N/A	N/A	N/A	N/A	N/A
	E-IAM-02	DCH-03_A07	access to CUI on system media is restricted to authorized personnel or roles.	
N/A	N/A	N/A	N/A	N/A
YES	E-AST-03 E-DCH-07	DCH-09_A08	system media that contain CUI are sanitized prior to disposal, release out of organizational control, or release for reuse.	
N/A	N/A	N/A	N/A	N/A
		DCH-04_A09	system media that contain CUI are marked to indicate distribution limitations.	
		DCH-04_A10	system media that contain CUI are marked to indicate handling caveats.	
		DCH-04_A11	system media that contain CUI are marked to indicate applicable CUI markings.	
N/A	N/A	N/A	N/A	N/A
		DCH-07_A12	system media that contain CUI are protected during transport outside of controlled areas.	
		DCH-07_A13	system media that contain CUI are controlled during transport outside of controlled areas.	
		DCH-07_A14	accountability for system media that contain CUI is maintained during transport outside of controlled areas.	
		DCH-07_A15	activities associated with the transport of system media that contain CUI are documented.	
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
		DCH-10_A03	types of system media with usage restrictions or that are prohibited from use are defined.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
		DCH-10_A08	the use of the following types of system media is restricted or prohibited: <A.03.08.07.ODP[01]: types of system media>.	US DoD ODP Value: any removable media not managed by or on behalf of the organization
		DCH-10.2_A02	the use of removable system media without an identifiable owner is prohibited.	
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
		BCD-11.4_A01	the confidentiality of backup information is protected.	
		BCD-11.4_A04	cryptographic mechanisms are implemented to prevent the unauthorized disclosure of CUI at backup storage locations.	
N/A	N/A	N/A	N/A	N/A
YES	E-HRS-17 E-HRS-21	HRS-04_A07	conditions that require the rescreening of individuals are defined.	
	E-HRS-17 E-HRS-21	HRS-04.1_A16	conditions that require the rescreening of individuals are defined.	
YES	E-HRS-17 E-HRS-21	HRS-04_A03	individuals are screened prior to authorizing access to the system.	
YES	E-HRS-17 E-HRS-21	HRS-04_A08	individuals are rescreened in accordance with the following conditions: <A.03.09.01.ODP[01]: conditions>.	US DoD ODP Value: an organizational policy requiring rescreening when there is a significant incident, or change in status, related to an individual
N/A	N/A	N/A	N/A	N/A
		HRS-08_A12	the time period within which to disable system access is defined.	
	E-HRS-19	HRS-09_A04	the time period within which to disable system access is defined.	
	E-HRS-19	HRS-09_A12	upon termination of individual employment, system access is disabled within <A.03.09.02.ODP[01]: time period>.	US DoD ODP Value: four (4) hours
	E-HRS-19	HRS-09_A06	upon termination of individual employment, authenticators associated with the individual are terminated or revoked.	
	E-HRS-19	HRS-09_A07	upon termination of individual employment, credentials associated with the individual are terminated or revoked.	
	E-AST-01	AST-10_A03	upon termination of individual employment, security-related system property is retrieved.	
	E-HRS-19	HRS-09_A09	upon termination of individual employment, security-related system property is retrieved.	
	E-HRS-19	HRS-09.1_A01	upon termination of individual employment, security-related system property is retrieved.	
YES	E-HRS-17 E-HRS-21	HRS-04_A09	upon individual reassignment or transfer to other positions in the organization, the ongoing operational need for current logical and physical access authorizations to the system and facility is reviewed.	
		HRS-08_A13	upon individual reassignment or transfer to other positions in the organization, the ongoing operational need for current logical and physical access authorizations to the system and facility is reviewed.	
		HRS-08_A14	upon individual reassignment or transfer to other positions in the organization, the ongoing operational need for current logical and physical access authorizations to the system and facility is confirmed.	
		HRS-08_A15	upon individual reassignment or transfer to other positions in the organization, access authorization is modified to correspond with any changes in operational need.	
N/A	N/A	N/A	N/A	N/A

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
	E-PES-03 E-PES-05	PES-02_A05	the frequency at which to review the access list detailing authorized facility access by individuals is defined.	
	E-PES-03 E-PES-05	PES-02.1_A03	the frequency at which to review the access list detailing authorized facility access by individuals is defined.	
	E-PES-03 E-PES-05	PES-02_A12	a list of individuals with authorized access to the facility where the system resides is developed.	
	E-PES-03 E-PES-05	PES-02_A06	a list of individuals with authorized access to the facility where the system resides is approved.	
	E-PES-03 E-PES-05	PES-02_A07	a list of individuals with authorized access to the facility where the system resides is maintained.	
	E-PES-03 E-PES-05	PES-02.1_A04	authorization credentials for facility access are issued.	
	E-PES-03 E-PES-05	PES-02_A14	the facility access list is reviewed <A.03.10.01.ODP[01]: frequency>.	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
	E-PES-03 E-PES-05	PES-02_A10	individuals from the facility access list are removed when access is no longer required.	
N/A	N/A	N/A	N/A	N/A
	E-PES-05	PES-05_A01	the frequency at which to review physical access logs is defined.	
	E-PES-05	PES-05_A02	events or potential indications of events requiring physical access logs to be reviewed are defined.	
	E-PES-05	PES-05_A03	physical access to the facility where the system resides is monitored to detect physical security incidents.	
	E-PES-05	PES-05_A08	physical security incidents are responded to.	
	E-PES-05	PES-05_A09	physical access logs are reviewed <A.03.10.02.ODP[01]: frequency>.	US DoD ODP Values: at least every 45 days
	E-PES-05	PES-05_A10	physical access logs are reviewed upon occurrence of <A.03.10.02.ODP[02]: events or potential indicators of events>.	US DoD ODP Values: significant, novel incidents, or significant changes to risks.
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
		PES-11_A02	security requirements to be employed at alternate work sites are defined.	
YES	E-NET-03	NET-14.5_A04	security requirements to be employed at alternate work sites are defined.	
		PES-11_A03	alternate work sites allowed for use by employees are determined.	
YES	E-NET-03	NET-14.5_A05	alternate work sites allowed for use by employees are determined.	
		PES-11_A09	the following security requirements are employed at alternate work sites: <A.03.10.06.ODP[01]: security requirements>.	US DoD ODP Value: adequate security, comparable to organizational security requirements at the primary work site where practical, documented in policy, and covered by training
YES	E-NET-03	NET-14.5_A06	the following security requirements are employed at alternate work sites: <A.03.10.06.ODP[01]: security requirements>.	US DoD ODP Value: adequate security, comparable to organizational security requirements at the primary work site where practical, documented in policy, and covered by training
N/A	N/A	N/A	N/A	N/A

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
	E-PES-03 E-PES-05	PES-02_A13	physical access authorizations are enforced at entry and exit points to the facility where the system resides by verifying individual physical access authorizations before granting access.	
YES	E-PES-05	PES-03_A02	physical access authorizations are enforced at entry and exit points to the facility where the system resides by controlling ingress and egress with physical access control systems, devices, or guards.	
	E-PES-02	PES-03.3_A01	physical access audit logs for entry or exit points are maintained.	
	E-PES-02	PES-06_A01	visitors are escorted.	
		PES-06.1_A02	visitors are escorted.	
YES		PES-06.3_A04	visitors are escorted.	
	E-PES-02	PES-06_A02	visitor activity is controlled.	
		PES-06.1_A03	visitor activity is controlled.	
YES		PES-06.1_A03	visitor activity is controlled.	
YES	E-PES-05	PES-03_A26	keys, combinations, and other physical access devices are secured.	
		PES-12.2_A03	physical access to output devices is controlled to prevent unauthorized individuals from obtaining access to CUI.	
N/A	N/A	N/A	N/A	N/A
		PES-12.1_A03	physical access to system distribution and transmission lines within organizational facilities is controlled.	
N/A	N/A	N/A	N/A	N/A
		RSK-07_A01	the frequency at which to update the risk assessment is defined.	
	E-RSK-01 E-RSK-06 E-RSK-07 E-RSK-08	RSK-01.1_A15	the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI is assessed.	
	E-RSK-04	RSK-03_A04	the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI is assessed.	
	E-RSK-09	RSK-03.1_A03	the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI is assessed.	
YES	E-RSK-04	RSK-04_A21	the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI is assessed.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
YES	E-RSK-02	RSK-09_A28	the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI is assessed.	
YES	E-RSK-04	RSK-04_A22	risk assessments are updated <A.03.11.01.ODP[01]: frequency>.	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
		RSK-07_A03	risk assessments are updated <A.03.11.01.ODP[01]: frequency>.	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
N/A	N/A	N/A	N/A	N/A
	E-VPM-05	VPM-06_A21	the frequency at which the system is monitored for vulnerabilities is defined.	
	E-VPM-05	VPM-06_A01	the frequency at which the system is scanned for vulnerabilities is defined.	
	E-MNT-03 E-THR-05 E-VPM-01	VPM-01_A16	response times to remediate system vulnerabilities are defined.	
YES	E-RSK-03 E-RSK-04 E-VPM-01	VPM-02_A02	response times to remediate system vulnerabilities are defined.	
	E-VPM-05	VPM-06_A17	the frequency at which to update system vulnerabilities to be scanned is defined.	
		VPM-06.1_A01	the frequency at which to update system vulnerabilities to be scanned is defined.	
	E-VPM-06	VPM-01.1_A09	the system is monitored for vulnerabilities <A.03.11.02.ODP[01]: frequency>.	US DoD ODP Value: at least monthly, or when there are significant incidents or significant changes to risks
	E-VPM-05	VPM-06_A22	the system is monitored for vulnerabilities <A.03.11.02.ODP[01]: frequency>.	US DoD ODP Value: at least monthly, or when there are significant incidents or significant changes to risks
	E-VPM-05	VPM-06_A23	the system is scanned for vulnerabilities <A.03.11.02.ODP[02]: frequency>.	US DoD ODP Value: at least monthly, or when there are significant incidents or significant changes to risks
	E-VPM-05	VPM-06_A12	the system is monitored for vulnerabilities when new vulnerabilities that affect the system are identified.	
	E-VPM-05	VPM-06_A13	the system is scanned for vulnerabilities when new vulnerabilities that affect the system are identified.	
	E-MNT-03 E-THR-05	VPM-04_A05	system vulnerabilities are remediated within <A.03.11.02.ODP[03]: response times>.	US DoD 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
YES	E-MNT-03	VPM-05_A15	system vulnerabilities are remediated within <A.03.11.02.ODP[03]: response times>.	US DoD 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
	E-VPM-05	VPM-06_A24	system vulnerabilities to be scanned are updated <A.03.11.02.ODP[04]: frequency>.	US DoD ODP Value: no more than 24 hours prior to running the scans
		VPM-06.1_A04	system vulnerabilities to be scanned are updated <A.03.11.02.ODP[04]: frequency>.	US DoD ODP Value: no more than 24 hours prior to running the scans
	E-VPM-05	VPM-06_A20	system vulnerabilities to be scanned are updated when new vulnerabilities are identified and reported.	
		VPM-06.1_A03	system vulnerabilities to be scanned are updated when new vulnerabilities are identified and reported.	
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
	E-RSK-03	RSK-06.1_A02	findings from security assessments are responded to.	
	E-RSK-03	RSK-06.1_A03	findings from security monitoring are responded to.	
	E-RSK-03	RSK-06.1_A04	findings from security audits are responded to.	
N/A	N/A	N/A	N/A	N/A
	E-CPL-04 E-CPL-07	CPL-02.1_A05	the frequency at which to assess the security requirements for the system and its environment of operation is defined.	
YES	E-CPL-05 E-CPL-07	CPL-03_A11	the security requirements for the system and its environment of operation are assessed <A.03.12.01.ODP[01]: frequency> to determine if the requirements have been satisfied.	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
N/A	N/A	N/A	N/A	N/A
	E-RSK-03	IAO-05_A24	a plan of action and milestones for the system is developed to document the planned remediation actions for correcting weaknesses or deficiencies noted during security assessments.	
	E-RSK-03	IAO-05_A25	a plan of action and milestones for the system is developed to reduce or eliminate known system vulnerabilities.	
	E-RSK-03	IAO-05_A26	the existing plan of action and milestones is updated based on the findings from security assessments.	
	E-RSK-03	IAO-05_A27	the existing plan of action and milestones is updated based on the findings from audits or reviews.	
	E-RSK-03	IAO-05_A28	the existing plan of action and milestones is updated based on the findings from continuous monitoring activities.	
N/A	N/A	N/A	N/A	N/A
YES	E-CPL-07 E-CPL-09 E-GOV-04 E-GOV-05 E-GOV-06 E-GOV-13 E-RSK-03	CPL-02_A29	a system-level continuous monitoring strategy is developed.	
	E-CPL-08	CPL-03.2_A05	a system-level continuous monitoring strategy is implemented.	
YES	E-CPL-07 E-CPL-09 E-GOV-04 E-GOV-05 E-GOV-06 E-GOV-13 E-RSK-03	CPL-02_A30	ongoing monitoring is included in the continuous monitoring strategy.	
YES	E-CPL-07 E-CPL-09 E-GOV-04 E-GOV-05 E-GOV-06 E-GOV-13 E-RSK-03	CPL-02_A31	security assessments are included in the continuous monitoring strategy.	
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
		NET-05_A17	one or more of the following PARAMETER VALUES are selected: {interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service-level agreements; user agreements; non-disclosure agreements; other types of agreements}.	
		NET-05_A04	the frequency at which to review and update agreements is defined.	
		NET-05_A18	the exchange of CUI between the system and other systems is approved using <A.03.12.05.ODP[01]: SELECTED PARAMETER VALUES>.	US DoD ODP Value: requirements as described in the contract
		NET-05_A19	the exchange of CUI between the system and other systems is managed using <A.03.12.05.ODP[01]: SELECTED PARAMETER VALUES>.	US DoD ODP Value: requirements as described in the contract
		NET-05_A07	interface characteristics for each system are documented as part of the exchange agreements.	
		NET-05_A02	security requirements for each system are documented as part of the exchange agreements.	
		NET-05_A08	responsibilities for each system are documented as part of the exchange agreements.	
		NET-05_A20	exchange agreements are reviewed <A.03.12.05.ODP[02]: frequency>.	US DoD ODP Value: at least every 12 months
		NET-05_A21	exchange agreements are updated <A.03.12.05.ODP[02]: frequency>.	US DoD ODP Value: at least every 12 months
N/A	N/A	N/A	N/A	N/A
	E-MON-01 E-MON-06 E-MON-07	MON-01.3_A08	communications at external managed interfaces to the system are monitored.	
YES		NET-03_A23	communications at external managed interfaces to the system are controlled.	
	E-MON-01 E-MON-06 E-MON-07	MON-01.3_A09	communications at key internal managed interfaces within the system are monitored.	
YES		NET-03_A24	communications at key internal managed interfaces within the system are controlled.	
YES		NET-06_A10	subnetworks are implemented for publicly accessible system components that are physically or logically separated from internal networks.	
YES		NET-03_A22	external system connections are only made through managed interfaces that consist of boundary protection devices arranged in accordance with an organizational security architecture.	
N/A	N/A	N/A	N/A	N/A

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
		SEA-05_A01	unauthorized information transfer via shared system resources is prevented.	
		SEA-05_A02	unintended information transfer via shared system resources is prevented.	
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
YES	E-AST-12 E-AST-19	NET-04.1_A01	network communications traffic is denied by default.	
YES	E-AST-12 E-AST-19	NET-04.1_A02	network communications traffic is allowed by exception.	
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
YES	E-CRY-01	CRY-01_A13	cryptographic mechanisms are implemented to prevent the unauthorized disclosure of CUI during transmission.	
YES	E-CRY-01	CRY-03_A04	cryptographic mechanisms are implemented to prevent the unauthorized disclosure of CUI during transmission.	
YES	E-CRY-01	CRY-01_A14	cryptographic mechanisms are implemented to prevent the unauthorized disclosure of CUI while in storage.	
YES	E-CRY-01	CRY-05_A08	cryptographic mechanisms are implemented to prevent the unauthorized disclosure of CUI while in storage.	
N/A	N/A	N/A	N/A	N/A
		NET-07_A05	the time period of inactivity after which the system terminates a network connection associated with a communications session is defined.	
		NET-07_A07	the network connection associated with a communications session is terminated at the end of the session or after <A.03.13.09.ODP[01]: time period> of inactivity.	US DoD ODP Value: no longer than 15 minutes
N/A	N/A	N/A	N/A	N/A
YES	E-CRY-01 E-CRY-02	CRY-09_A01	requirements for key generation, distribution, storage, access, and destruction are defined.	
YES	E-CRY-01 E-CRY-02	CRY-09_A05	cryptographic keys are established in the system in accordance with the following key management requirements: <A.03.13.10.ODP[01]: requirements>.	US DoD ODP Value: Guidance: At a minimum, establish a policy and procedure in line with the latest Cryptographic key management guidance
YES	E-CRY-01 E-CRY-02	CRY-09_A06	cryptographic keys are managed in the system in accordance with the following key management requirements: <A.03.13.10.ODP[01]: requirements>.	US DoD ODP Value: Guidance: At a minimum, establish a policy and procedure in line with the latest Cryptographic key management guidance
N/A	N/A	N/A	N/A	N/A
YES	E-CRY-01	CRY-01_A15	the types of cryptography for protecting the confidentiality of CUI are defined.	
YES	E-CRY-01	CRY-03_A05	the types of cryptography for protecting the confidentiality of CUI are defined.	
YES	E-CRY-01	CRY-05_A09	the types of cryptography for protecting the confidentiality of CUI are defined.	
YES	E-CRY-01	CRY-01_A16	the following types of cryptography are implemented to protect the confidentiality of CUI: <A.03.13.11.ODP[01]: types of cryptography>.	US DoD ODP Value: FIPS Validated Cryptography (https://csrc.nist.gov/Projects/Cryptographic-ModuleValidation-Program/Validated-Modules)

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
YES	E-CRY-01	CRY-03_A06	the following types of cryptography are implemented to protect the confidentiality of CUI: <A.03.13.11.ODP[01]: types of cryptography>.	US DoD ODP Value: FIPS Validated Cryptography (https://csrc.nist.gov/Projects/Cryptographic-ModuleValidation-Program/Validated-Modules)
YES	E-CRY-01	CRY-05_A10	the following types of cryptography are implemented to protect the confidentiality of CUI: <A.03.13.11.ODP[01]: types of cryptography>.	US DoD ODP Value: FIPS Validated Cryptography (https://csrc.nist.gov/Projects/Cryptographic-ModuleValidation-Program/Validated-Modules)
N/A	N/A	N/A	N/A	N/A
		END-14_A04	exceptions where remote activation is to be allowed are defined.	
		END-14_A09	the remote activation of collaborative computing devices and applications is prohibited with the following exceptions: <A.03.13.12.ODP[01]: exceptions>.	US DoD 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
		END-14.6_A01	an explicit indication of use is provided to users who are physically present at the devices.	
N/A	N/A	N/A	N/A	N/A
		END-10_A18	acceptable mobile code is defined.	
		END-10_A01	acceptable mobile code technologies are defined.	
		END-10_A19	the use of mobile code is authorized.	
		END-10_A20	the use of mobile code is monitored.	
		CFG-03.3_A17	the use of mobile code is controlled.	
		END-10_A21	the use of mobile code is controlled.	
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
		NET-09_A01	the authenticity of communications sessions is protected.	
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
YES	E-MNT-03	VPM-05_A01	the time period within which to install security-relevant software updates after the release of the updates is defined.	
YES	E-MNT-03	VPM-05_A14	the time period within which to install security-relevant firmware updates after the release of the updates is defined.	
YES	E-MNT-03	VPM-05_A02	system flaws are identified.	
YES	E-MNT-03	VPM-05_A05	system flaws are reported.	
YES	E-MNT-03	VPM-05_A04	system flaws are corrected.	
YES	E-MNT-03	VPM-05_A16	security-relevant software updates are installed within <A.03.14.01.ODP[01]: time period> of the release of the updates.	US DoD 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
YES	E-MNT-03	VPM-05_A17	security-relevant firmware updates are installed within <A.03.14.01.ODP[02]: time period> of the release of the updates.	US DoD 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
N/A	N/A	N/A	N/A	N/A
YES	E-AST-27 E-MON-02	END-04_A19	the frequency at which malicious code protection mechanisms perform scans is defined.	
YES	E-AST-27 E-MON-02	END-04_A08	malicious code protection mechanisms are implemented at system entry and exit points to detect malicious code.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
YES	E-AST-27 E-MON-02	END-04_A09	malicious code protection mechanisms are implemented at system entry and exit points to eradicate malicious code.	
		END-04.1_A02	malicious code protection mechanisms are updated as new releases are available in accordance with configuration management policy and procedures.	
		END-04.7_A04	malicious code protection mechanisms are configured to perform scans of the system <A.03.14.02.ODP[01]: frequency>.	US DoD ODP Value: at least weekly
		END-04.7_A03	malicious code protection mechanisms are configured to perform real-time scans of files from external sources at endpoints or system entry and exit points as the files are downloaded, opened, or executed.	
YES	E-AST-27 E-MON-02	END-04_A18	malicious code protection mechanisms are configured to block malicious code, quarantine malicious code, or take other actions in response to malicious code detection.	
N/A	N/A	N/A	N/A	N/A
	E-THR-03	THR-03_A05	system security alerts, advisories, and directives from external organizations are received on an ongoing basis.	
		THR-03.1_A01	internal security alerts, advisories, and directives are generated, as necessary.	
		THR-03.1_A02	internal security alerts, advisories, and directives are disseminated, as necessary.	
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
YES	E-MON-01 E-MON-06 E-MON-07	MON-01_A09	the system is monitored to detect attacks.	
YES	E-MON-01 E-MON-06 E-MON-07	MON-01_A10	the system is monitored to detect indicators of potential attacks.	
YES	E-MON-01 E-MON-06 E-MON-07	MON-01_A11	the system is monitored to detect unauthorized connections.	
YES	E-IRO-02 E-MON-07	MON-16_A08	unauthorized use of the system is identified.	
	E-MON-01 E-MON-06 E-MON-07	MON-01.3_A04	inbound communications traffic is monitored to detect unusual or unauthorized activities or conditions.	
	E-MON-01 E-MON-06 E-MON-07	MON-01.3_A05	outbound communications traffic is monitored to detect unusual or unauthorized activities or conditions.	
N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A
	E-AST-11	DCH-18_A09	CUI within the system is managed in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.	
	E-AST-11	DCH-18_A10	CUI within the system is retained in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.	
	E-AST-11	DCH-18_A11	CUI output from the system is managed in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
	E-AST-11	DCH-18_A12	CUI output from the system is retained in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.	
N/A	N/A	N/A	N/A	N/A
	E-GOV-12	GOV-03_A01	the frequency at which the policies and procedures for satisfying security requirements are reviewed and updated is defined.	
YES	E-GOV-08 E-GOV-09 E-GOV-11	GOV-02_A18	policies needed to satisfy the security requirements for the protection of CUI are developed and documented.	
YES	E-GOV-08 E-GOV-09 E-GOV-11	GOV-02_A19	policies needed to satisfy the security requirements for the protection of CUI are disseminated to organizational personnel or roles.	
YES	E-GOV-08 E-GOV-09 E-GOV-11	GOV-02_A20	procedures needed to satisfy the security requirements for the protection of CUI are developed and documented.	
	E-GOV-11	OPS-01.1_A11	procedures needed to satisfy the security requirements for the protection of CUI are developed and documented.	
YES	E-GOV-08 E-GOV-09 E-GOV-11	GOV-02_A21	procedures needed to satisfy the security requirements for the protection of CUI are disseminated to organizational personnel or roles.	
	E-GOV-11	OPS-01.1_A12	procedures needed to satisfy the security requirements for the protection of CUI are disseminated to organizational personnel or roles.	
	E-GOV-12	GOV-03_A04	policies and procedures are reviewed <A.03.15.01.ODP[01]: frequency>.	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
	E-GOV-11	OPS-01.1_A13	policies and procedures are reviewed <A.03.15.01.ODP[01]: frequency>.	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
	E-GOV-12	GOV-03_A05	policies and procedures are updated <A.03.15.01.ODP[01]: frequency>.	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
	E-GOV-11	OPS-01.1_A14	policies and procedures are updated <A.03.15.01.ODP[01]: frequency>.	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
N/A	N/A	N/A	N/A	N/A
	E-TDA-14	IAO-03_A20	the frequency at which the system security plan is reviewed and updated is defined.	
	E-TDA-14	IAO-03_A24	a system security plan that defines the constituent system components is developed.	
	E-TDA-14	IAO-03_A30	a system security plan that identifies the information types processed, stored, and transmitted by the system is developed.	
	E-TDA-14	IAO-03_A06	a system security plan that describes specific threats to the system that are of concern to the organization is developed.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
	E-TDA-14	IAO-03_A38	a system security plan that describes the operational environment for the system and any dependencies on or connections to other systems or system components is developed.	
	E-TDA-14	IAO-03_A39	a system security plan that provides an overview of the security requirements for the system is developed.	
	E-TDA-14	IAO-03_A07	a system security plan that describes the safeguards in place or planned for meeting the security requirements is developed.	
	E-TDA-14	IAO-03_A08	a system security plan that identifies individuals that fulfill system roles and responsibilities is developed.	
	E-TDA-14	IAO-03_A63	a system security plan that includes other relevant information necessary for the protection of CUI is developed.	
	E-TDA-14	IAO-03_A64	the system security plan is reviewed <A.03.15.02.ODP[01]: frequency>.	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
	E-TDA-14	IAO-03_A65	the system security plan is updated <A.03.15.02.ODP[01]: frequency>.	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
	E-DCH-02 E-DCH-08	DCH-01.4_A03	the system security plan is protected from unauthorized disclosure.	
YES		DCH-03.1_A03	the system security plan is protected from unauthorized disclosure.	
	E-TDA-14	IAO-03_A11	the system security plan is protected from unauthorized disclosure.	
N/A	N/A	N/A	N/A	N/A
YES	E-HRS-22	HRS-05.1_A03	the frequency at which the rules of behavior are reviewed and updated is defined.	
YES	E-HRS-22	HRS-05.1_A07	rules that describe responsibilities and expected behavior for system usage and protecting CUI are established.	
	E-HRS-22	HRS-05.2_A05	rules that describe responsibilities and expected behavior for system usage and protecting CUI are established.	
YES	E-HRS-22	HRS-05.3_A03	rules that describe responsibilities and expected behavior for system usage and protecting CUI are established.	
	E-HRS-22	HRS-05.5_A03	rules that describe responsibilities and expected behavior for system usage and protecting CUI are established.	
YES	E-HRS-16 E-HRS-22	HRS-05_A02	rules are provided to individuals who require access to the system.	
	E-HRS-18 E-SAT-02 E-SAT-04	HRS-05.7_A03	a documented acknowledgement from individuals indicating that they have read, understand, and agree to abide by the rules of behavior is received before authorizing access to CUI and the system.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
YES	E-HRS-22	HRS-05.1_A08	the rules of behavior are reviewed <A.03.15.03.ODP[01]: frequency>.	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
YES	E-HRS-22	HRS-05.1_A09	the rules of behavior are updated <A.03.15.03.ODP[01]: frequency>.	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
N/A	N/A	N/A	N/A	N/A
YES	E-TDA-01 E-TDA-02 E-TDA-04 E-TDA-08 E-TDA-09	SEA-01_A07	systems security engineering principles to be applied to the development or modification of the system and system components are defined.	
YES	E-TDA-01 E-TDA-02 E-TDA-08	TDA-01_A31	systems security engineering principles to be applied to the development or modification of the system and system components are defined.	
	E-TDA-04	TDA-02.3_A06	systems security engineering principles to be applied to the development or modification of the system and system components are defined.	
		GOV-15_A04	<A.03.16.01.ODP[01]: systems security engineering principles> are applied to the development or modification of the system and system components.	US DoD 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.
	E-TDA-04	TDA-02.3_A07	<A.03.16.01.ODP[01]: systems security engineering principles> are applied to the development or modification of the system and system components.	US DoD 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.
N/A	N/A	N/A	N/A	N/A
YES	E-AST-09	TDA-17_A02	system components are replaced when support for the components is no longer available from the developer, vendor, or manufacturer.	
		TDA-17.1_A01	options for risk mitigation or alternative sources for continued support for unsupported components that cannot be replaced are provided.	
N/A	N/A	N/A	N/A	N/A
YES	E-RSK-02 E-TPM-01 E-TPM-03	TPM-05_A03	security requirements to be satisfied by external system service providers are defined.	
	E-RSK-02	TPM-05.2_A02	security requirements to be satisfied by external system service providers are defined.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
YES	E-RSK-02 E-TPM-01 E-TPM-03	TPM-05_A05	the providers of external system services used for the processing, storage, or transmission of CUI comply with the following security requirements: <A.03.16.03.ODP[01]: security requirements>.	US DoD ODP Values: (1) For cloud service providers: (i) FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline in accordance with the FedRAMP Marketplace; or (ii) meets security requirements established by the government equivalent to the FedRAMP Moderate (or higher) baseline. (2) All other external service providers must meet NIST SP 800-171 R2.
	E-CPL-03	TPM-05.4_A02	user roles and responsibilities with regard to external system services, including shared responsibilities with external service providers, are defined and documented.	
YES	E-TPM-03	TPM-05.5_A02	processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis are implemented.	
	E-TPM-01	TPM-05.6_A02	processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis are implemented.	
		TPM-05.8_A03	processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis are implemented.	
	E-TPM-03	TPM-08_A05	processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis are implemented.	
N/A	N/A	N/A	N/A	N/A
YES	E-RSK-02	RSK-09_A07	the frequency at which to review and update the supply chain risk management plan is defined.	
YES	E-RSK-02	RSK-09_A04	a plan for managing supply chain risks is developed.	
YES	E-RSK-02	RSK-09_A09	the SCRM plan addresses risks associated with the research and development of the system, system components, or system services.	
YES	E-RSK-02	RSK-09_A10	the SCRM plan addresses risks associated with the design of the system, system components, or system services.	
YES	E-RSK-02	RSK-09_A11	the SCRM plan addresses risks associated with the manufacturing of the system, system components, or system services.	
YES	E-RSK-02	RSK-09_A12	the SCRM plan addresses risks associated with the acquisition of the system, system components, or system services.	

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
YES	E-RSK-02	RSK-09_A13	the SCRM plan addresses risks associated with the delivery of the system, system components, or system services.	
YES	E-RSK-02	RSK-09_A14	the SCRM plan addresses risks associated with the integration of the system, system components, or system services.	
YES	E-RSK-02	RSK-09_A15	the SCRM plan addresses risks associated with the operation of the system, system components, or system services.	
YES	E-RSK-02	RSK-09_A16	the SCRM plan addresses risks associated with the maintenance of the system, system components, or system services.	
YES	E-RSK-02	RSK-09_A17	the SCRM plan addresses risks associated with the disposal of the system, system components, or system services.	
YES	E-RSK-02	RSK-09_A29	the SCRM plan is reviewed <A.03.17.01.ODP[01]: frequency>.	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
YES	E-RSK-02	RSK-09_A30	the SCRM plan is updated <A.03.17.01.ODP[01]: frequency>.	US DoD ODP Value: at least every 12 months, or when there are significant incidents or significant changes to risks
	E-DCH-02 E-DCH-08	DCH-01.4_A04	the SCRM plan is protected from unauthorized disclosure.	
YES		DCH-03.1_A04	the SCRM plan is protected from unauthorized disclosure.	
YES	E-RSK-02	RSK-09_A20	the SCRM plan is protected from unauthorized disclosure.	
N/A	N/A	N/A	N/A	N/A
		TPM-03.1_A03	acquisition strategies, contract tools, and procurement methods are developed to identify supply chain risks.	
		TPM-03.1_A04	acquisition strategies, contract tools, and procurement methods are developed to protect against supply chain risks.	
		TPM-03.1_A05	acquisition strategies, contract tools, and procurement methods are developed to mitigate supply chain risks.	
YES	E-TDA-01 E-TDA-02 E-TDA-08	TDA-01_A03	acquisition strategies, contract tools, and procurement methods are implemented to identify supply chain risks.	
YES	E-TDA-01 E-TDA-02 E-TDA-08	TDA-01_A04	acquisition strategies, contract tools, and procurement methods are implemented to protect against supply chain risks.	
YES	E-TDA-01 E-TDA-02 E-TDA-08	TDA-01_A05	acquisition strategies, contract tools, and procurement methods are implemented to mitigate supply chain risks.	
N/A	N/A	N/A	N/A	N/A

Material Control	Evidence Request List (ERL) #	AO #	SCF Assessment Objective (AO)	Notes
YES	E-RSK-02	RSK-09_A05	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 are defined.	
YES	E-TPM-03	TPM-01_A01	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 are defined.	
YES	E-RSK-02	RSK-09_A25	a process for identifying weaknesses or deficiencies in the supply chain elements and processes is established.	
	E-TPM-01 E-TPM-02 E-TPM-03	TPM-04.1_A04	a process for identifying weaknesses or deficiencies in the supply chain elements and processes is established.	
YES	E-RSK-02	RSK-09_A27	a process for addressing weaknesses or deficiencies in the supply chain elements and processes is established.	
YES	E-RSK-01	RSK-01_A12	the following security requirements are enforced to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences of supply chain-related events: <A.03.17.03.ODP[01]: security requirements>.	US DoD 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
YES	E-RSK-02	RSK-09_A31	the following security requirements are enforced to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences of supply chain-related events: <A.03.17.03.ODP[01]: security requirements>.	US DoD 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