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: **Department of War (DoW) - Zero Trust Execution Roadmap (v1.1)**
Focal Document URL: https://dodcio.defense.gov/Portals/0/Documents/Library/ZT-CapabilitiesActivities.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-dow-zt-roadmap-1-1.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1	User	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No applicable SCF control
1.1	User Inventory	Regular and Privileged users are identified and integrated into an inventory supporting regular modifications. Applications, software and services that have local users are all part of the inventory and highlighted.	Functional	Subset Of	User & Service Account Inventories	IAC-01.3	Mechanisms exist to maintain a current list of authorized users and service accounts.	10	
1.1.1	Inventory User	DoD Components utilize Enterprise authoritative source of (PE/NPE) identity (PE - AMID, NIS, AFID) and/or establish or augment with local authoritative source. Identity management can be done manually if needed, preparing for automated approach in later stages. Identity source is connected to identity life cycle management processes (i.e. joiner/mover/leaver/returner). IT privileged users are clearly identified.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
1.1.1	Inventory User	DoD Components utilize Enterprise authoritative source of (PE/NPE) identity (PE - AMID, NIS, AFID) and/or establish or augment with local authoritative source. Identity management can be done manually if needed, preparing for automated approach in later stages. Identity source is connected to identity life cycle management processes (i.e. joiner/mover/leaver/returner). IT privileged users are clearly 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).	8	
1.1.1	Inventory User	DoD Components utilize Enterprise authoritative source of (PE/NPE) identity (PE - AMID, NIS, AFID) and/or establish or augment with local authoritative source. Identity management can be done manually if needed, preparing for automated approach in later stages. Identity source is connected to identity life cycle management processes (i.e. joiner/mover/leaver/returner). IT privileged users are clearly identified.	Functional	Intersects With	Identity Proofing (Identity Verification)	IAC-28	Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions.	3	
1.2	Conditional User Access	Through maturity levels Conditional Access works to create a dynamic level of access for users in the environment. This starts with traditional role based access controls across a federate ICAM, expands to be application focused roles and ultimately utilizes enterprise attributes to provide dynamic access rules.	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	
1.2	Conditional User Access	Through maturity levels Conditional Access works to create a dynamic level of access for users in the environment. This starts with traditional role based access controls across a federate ICAM, expands to be application focused roles and ultimately utilizes enterprise attributes to provide dynamic access rules.	Functional	Intersects With	Attribute-Based Access Control (ABAC)	IAC-29	Mechanisms exist to enforce Attribute-Based Access Control (ABAC) for policy-driven, dynamic authorizations that supports the secure sharing of information.	8	
1.2.1	Implement App Based Permissions per Enterprise	The DoD ICAM governance establishes a set of user attributes for authentication and authorization. These are integrated with the "Enterprise Identity Life-Cycle Management Pt1" activity process for a complete Enterprise standard. The Enterprise Identity, Credential and Access Management (ICAM) solution are enabled for adding/updating attributes within the solution to better support identity federation. Remaining Privileged Access Management (PAM) activities are approved and tailored as specified by roles.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	8	
1.2.1	Implement App Based Permissions per Enterprise	The DoD ICAM governance establishes a set of user attributes for authentication and authorization. These are integrated with the "Enterprise Identity Life-Cycle Management Pt1" activity process for a complete Enterprise standard. The Enterprise Identity, Credential and Access Management (ICAM) solution are enabled for adding/updating attributes within the solution to better support identity federation. Remaining Privileged Access Management (PAM) activities are approved and tailored as specified by roles.	Functional	Intersects With	Attribute-Based Access Control (ABAC)	IAC-29	Mechanisms exist to enforce Attribute-Based Access Control (ABAC) for policy-driven, dynamic authorizations that supports the secure sharing of information.	8	
1.2.1	Implement App Based Permissions per Enterprise	The DoD ICAM governance establishes a set of user attributes for authentication and authorization. These are integrated with the "Enterprise Identity Life-Cycle Management Pt1" activity process for a complete Enterprise standard. The Enterprise Identity, Credential and Access Management (ICAM) solution are enabled for adding/updating attributes within the solution to better support identity federation. Remaining Privileged Access Management (PAM) activities are approved and tailored as specified by roles.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	
1.2.2	Rule Based Dynamic Access Pt1	DoD Components utilize the rules from the "Periodic Authentication" activity to build rules enabling and disabling privileges dynamically. IT Privileged user accounts utilize the PAM solution to move to dynamic privileged access using Just-in-Time (JIT) access and Just-Enough- Administration (JEA) methods.	Functional	Intersects With	Attribute-Based Access Control (ABAC)	IAC-29	Mechanisms exist to enforce Attribute-Based Access Control (ABAC) for policy-driven, dynamic authorizations that supports the secure sharing of information.	8	
1.2.2	Rule Based Dynamic Access Pt1	DoD Components utilize the rules from the "Periodic Authentication" activity to build rules enabling and disabling privileges dynamically. IT Privileged user accounts utilize the PAM solution to move to dynamic privileged access using Just-in-Time (JIT) access and Just-Enough- Administration (JEA) methods.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	8	
1.2.3	Rule Based Dynamic Access Pt2	DoD Components expand the development of rules for dynamic access decision making accounting for risk. Solutions used for dynamic access are integrated with cross pillar Machine Learning (ML) and Artificial Intelligence (AI) functionality enabling automated rule management.	Functional	Subset Of	Attribute-Based Access Control (ABAC)	IAC-29	Mechanisms exist to enforce Attribute-Based Access Control (ABAC) for policy-driven, dynamic authorizations that supports the secure sharing of information.	10	
1.2.4	Enterprise Gov't roles and Permissions Pt1	DoD Components federate remaining user and group attributes as appropriate to the Enterprise Identity, Credential and Access Management (ICAM) solution. The updated attribute set is used to create universal roles for Organizations to use. Core functions of the Identity Provider (IdP) and ICAM solutions are migrated to cloud services and/or environments enabling improved resilience and performance.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
1.2.5	Enterprise Gov't roles and Permissions Pt2	DoD Components move all possible functions of the Identity Provider (IdP) and Identity, Credential and Access Management (ICAM) solutions to cloud environments. Enclave/Denied, Disrupted, Intermittent, and Limited (DDIL) environments utilize local capabilities to support disconnected functions but ultimately are managed by the centralized ICAM. Updated roles are now mandated for usage and exceptions are reviewed following a risk-based approach.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
1.3	Multi-Factor Authentication (MFA)	This capability initially focuses on developing an organization focused MFA provider and Identity Provider to enable the centralization of users. Retirement of local and/or built-in accounts and groups is a critical piece to this capability. At the later maturity levels alternative and flexible MFA tokens can be used to provide access for standard and external users.	Functional	Equal	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.	10	
1.3.1	Organizational MFA/IDP	DoD Components or Identity Provider (IdP) solution using approved credential or approved alternative Multi-Factor Authentication (MFA). The IdP and MFA solution may be combined in a single application or separated as needed assuming automated integration is supported by both solutions. Both IdP and MFA support integration with the Enterprise PKI capability as well as enabling key pairs to be signed by the trusted root certificate authorities. Authentication for mission/task-critical applications and services authentication is MFA-Enabled and leverages the related authentication mechanisms to manage users and groups.	Functional	Subset Of	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.	10	
1.3.2	Alternative Flexible MFA Pt1	DoD Components Identity Provider (IdP) supports alternative methods of Multi-Factor Authentication (MFA) complying with Cyber Security requirements (e.g., FIPS 140-2, FIPS 197, etc.). Alternative tokens can be used for application-based authentication. MFA options support biometric capability and can be managed using a self-service approach. Where possible MFA provider(s) are moved to cloud services instead of being hosted on-premise.	Functional	Equal	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.	10	
1.3.3	Alternative Flexible MFA Pt2	Alternative Multi-Factor Authentication (MFA) methods utilize user activity patterns from cross pillar activities such as "User Activity Monitoring (UAM) and User & Entity Behavior Analytics (UEBA)" to assist with access decision making (e.g., not grant access when pattern deviation occurs).	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	
1.3.3	Alternative Flexible MFA Pt2	Alternative Multi-Factor Authentication (MFA) methods utilize user activity patterns from cross pillar activities such as "User Activity Monitoring (UAM) and User & Entity Behavior Analytics (UEBA)" to assist with access decision making (e.g., not grant access when pattern deviation occurs).	Functional	Intersects With	Attribute-Based Access Control (ABAC)	IAC-29	Mechanisms exist to enforce Attribute-Based Access Control (ABAC) for policy-driven, dynamic authorizations that supports the secure sharing of information.	8	
1.4	Privileged Access Management (PAM)	The capability focuses on removal of permanent administrator/elevated privileges by first creating a Privileged Account Management (PAM) system and migrating privileged users to it. The capability is then expanded upon by using automation with privilege escalation approvals and feeding analytics into the system for anomaly detection.	Functional	Subset Of	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	10	
1.4.1	Implement System and Migrate Privileged Users Pt1	DoD Components procure and implement a Privileged Access Management (PAM) solution to support all critical privileged use cases. Application/Service integration points are identified to determine status of support for the PAM solution. Applications/Services that easily integrate with the PAM solution are transitioned to using the solution versus static and direct privileged permissions.	Functional	Subset Of	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	10	
1.4.2	Implement System and Migrate Privileged Users Pt2	DoD Components utilize the inventory of supported and unsupported Applications/Services for integration with the Privileged Access Management (PAM) solution to extend integrations. PAM is integrated with the more challenging Applications/Services to maximize PAM solution coverage. Exceptions are managed in a risk-based methodical approach with the goal of migration off and/or decommissioning Applications/Services that do not support the PAM solution.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	8	
1.4.2	Implement System and Migrate Privileged Users Pt2	DoD Components utilize the inventory of supported and unsupported Applications/Services for integration with the Privileged Access Management (PAM) solution to extend integrations. PAM is integrated with the more challenging Applications/Services to maximize PAM solution coverage. Exceptions are managed in a risk-based methodical approach with the goal of migration off and/or decommissioning Applications/Services that do not support the PAM solution.	Functional	Intersects With	Attribute-Based Access Control (ABAC)	IAC-29	Mechanisms exist to enforce Attribute-Based Access Control (ABAC) for policy-driven, dynamic authorizations that supports the secure sharing of information.	8	
1.4.3	Real time Approvals & JIT/JEA Analytics Pt1	Identification of necessary attributes (Users, Groups, etc.) are automated and integrated into the Privileged Access Management (PAM) solution. Privilege access requests are migrated to the PAM solution for automated approvals and denials.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	8	
1.4.4	Real time Approvals & JIT/JEA Analytics Pt2	DoD Components integrate User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions with the Privileged Access Management (PAM) solution providing user pattern analytics for decision making.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1.4.4	Real time Approvals & JIT/JEA Analytics Pt2	DoD Components integrate User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions with the Privileged Access Management (PAM) solution providing user pattern analytics for decision making.	Functional	Intersects With	Attribute-Based Access Control (ABAC)	IAC-29	Mechanisms exist to enforce Attribute-Based Access Control (ABAC) for policy-driven, dynamic authorizations that supports the secure sharing of information.	8	
1.5	Identity Federation & User Credentialing	The initial scope of this capability focuses on standardizing the Identity Lifecycle Management (ILM) processes and integrating with the standard organizational IDP/IDM solution. Once completed the capability shifts to establishing an Enterprise ILM process/solution either through a single solution or identity federation.	Functional	Equal	Federated Credential Management	IAC-13.2	Mechanisms exist to federate credentials to allow cross-organization authentication of individuals and devices.	10	
1.5.1	Organizational Identity Life-Cycle Management	DoD Components establish a process for life cycle management of users both privileged and non-privileged. Utilizing an approved Identity Provider (IdP) the process is implemented and followed by the maximum number of users. Users falling outside of the standard process are approved through risk-based exceptions to be evaluated regularly for decommission.	Functional	Intersects With	Federated Credential Management	IAC-13.2	Mechanisms exist to federate credentials to allow cross-organization authentication of individuals and devices.	5	
1.5.2	Enterprise Identity Life-Cycle Management Pt 1	Specified policies and supporting process are followed by DoD Components. DoD Components implement the Enterprise Identity Life- Cycle Management process for the maximum number of identities, attributes, groups, credentials, and permissions. Exceptions to the policy are managed in a risk-based methodical approach.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
1.5.3	Enterprise Identity LifeCycle Management Pt2	DoD Components further integrate the critical automation functions of the Identity Provider (IdP) and Identity, Credential and Access Management (ICAM) solutions following the Enterprise Identity Life- Cycle Management (ILM) process to enable Enterprise automation and analytics. ILM primary processes are integrated into the cloud-based Enterprise ICAM solution.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
1.5.4	Enterprise Identity LifeCycle Management Pt3	DoD Components integrate remaining Identity Lifecycle Management (ILM) processes with the Enterprise Identity, Credential and Access Management (ICAM) solution. Enclave/DDIL environments, while still authorized to operate, integrate with the Enterprise ICAM using local connectors to the cloud environment.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
1.6	Behavioral, Contextual ID, and Biometrics	Utilizing the Enterprise IDP, user and entity behavioral analytics (UEBA) are enabled with basic user attributes. Once completed this is expanded into Organizational specific attributes using Organizational IDPs as available. Finally UEBA are integrated with the PAM and JIT/JEA systems to better detect anomalous and malicious activities.	Functional	Intersects With	Dynamic Attribute Association	DCH-05.1	Mechanisms exist to dynamically associate cybersecurity and data protection attributes with individuals and objects as information is created, combined, or transformed, in accordance with organization-defined cybersecurity and data protection policies.	3	
1.6	Behavioral, Contextual ID, and Biometrics	Utilizing the Enterprise IDP, user and entity behavioral analytics (UEBA) are enabled with basic user attributes. Once completed this is expanded into Organizational specific attributes using Organizational IDPs as available. Finally UEBA are integrated with the PAM and JIT/JEA systems to better detect anomalous and malicious activities.	Functional	Intersects With	Attribute-Based Access Control (ABAC)	IAC-29	Mechanisms exist to enforce Attribute-Based Access Control (ABAC) for policy-driven, dynamic authorizations that supports the secure sharing of information.	8	
1.6.1	Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling	DoD Components procure and implement User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions. Initial integration point with Enterprise IdP is completed, enabling future usage in decision making.	Functional	Equal	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	10	
1.6.2	User Activity Monitoring Pt1	DoD Components integrate User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions with Identity Providers (IdP) for extended visibility as needed. Analytics and data generated by UEBA and UAM for critical applications/services are integrated with Just-in- Time (JIT) and Just-Enough-Access (JEA) solutions for improving decision.	Functional	Intersects With	Attribute-Based Access Control (ABAC)	IAC-29	Mechanisms exist to enforce Attribute-Based Access Control (ABAC) for policy-driven, dynamic authorizations that supports the secure sharing of information.	8	
1.6.2	User Activity Monitoring Pt1	DoD Components integrate User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions with Identity Providers (IdP) for extended visibility as needed. Analytics and data generated by UEBA and UAM for critical applications/services are integrated with Just-in- Time (JIT) and Just-Enough-Access (JEA) solutions for improving decision.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	8	
1.6.3	User Activity Monitoring Pt2	DoD Components continue the analytics usage from User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions by using generated data for all monitored applications and services when decision making occurs in the Just-in-Time (JIT) and Just-Enough- Access (JEA) solution.	Functional	Intersects With	Attribute-Based Access Control (ABAC)	IAC-29	Mechanisms exist to enforce Attribute-Based Access Control (ABAC) for policy-driven, dynamic authorizations that supports the secure sharing of information.	8	
1.6.3	User Activity Monitoring Pt2	DoD Components continue the analytics usage from User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions by using generated data for all monitored applications and services when decision making occurs in the Just-in-Time (JIT) and Just-Enough- Access (JEA) solution.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	8	
1.7	Least Privileged Access	DoD organizations govern access to DAAS using the absolute minimum access required to perform routine, legitimate tasks or activities. DoD Application Owners identify the necessary roles and attributes for standard and privileged user access. Privileged access for all DoD organization DAAS is audited and removed when unneeded.	Functional	Equal	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	10	
1.7.1	Deny User by Default Policy	DoD Components audit user and group usage for permissions and revoke permissions when appropriate. This activity includes the revocation and/or decommission of excess permissions and access for application/service-based identities and groups. Where possible, static privileged users are decommissioned or permission are reduced, preparing for future rule/dynamic based access. The implemented audit and governance functions are automated where possible.	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	
1.8	Continuous Authentication	The DoD organizations and overall enterprise will methodically move towards continuous attribute based authentication. Initially the ˙capability focuses on standardizing legacy single authentication to a organizationally approved IDP with users and groups. The second stages adds in based rule based (time) authentication and ultimately matures to Continuous Authentication based on the application/software activities and privileges requested.	Functional	Subset Of	Continuous Authentication	IAC-13.3	Automated mechanisms exist to enable continuous re-authentication through the lifecycle of entity interactions.	10	
1.8	Continuous Authentication	The DoD organizations and overall enterprise will methodically move towards continuous attribute based authentication. Initially the ˙capability focuses on standardizing legacy single authentication to a organizationally approved IDP with users and groups. The second stages adds in based rule based (time) authentication and ultimately matures to Continuous Authentication based on the application/software activities and privileges requested.	Functional	Intersects With	Attribute-Based Access Control (ABAC)	IAC-29	Mechanisms exist to enforce Attribute-Based Access Control (ABAC) for policy-driven, dynamic authorizations that supports the secure sharing of information.	8	
1.8.1	Single Authentication	DoD Components authenticate users and NPEs at least once per session (e.g., logon) using CAC and other DoD approved methods. Users being authenticated are managed by the parallel activity “Organizational MFA/IdP” with the Component Identity Provider (IdP). Components do not use application/service-based identities and groups.	Functional	Intersects With	Acceptance of PIV Credentials	IAC-02.3	Mechanisms exist to accept and electronically verify organizational Personal Identity Verification (PIV) credentials.	8	
1.8.1	Single Authentication	DoD Components authenticate users and NPEs at least once per session (e.g., logon) using CAC and other DoD approved methods. Users being authenticated are managed by the parallel activity “Organizational MFA/IdP” with the Component Identity Provider (IdP). Components do not use application/service-based identities and groups.	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	
1.8.2	Periodic Authentication	DoD Components enable periodic authentication for applications and services. Traditionally, these are based on duration and/or duration timeout, however, other period-based analytics can be used to enforce re-authentication of user 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.	8	
1.8.2	Periodic Authentication	DoD Components enable periodic authentication for applications and services. Traditionally, these are based on duration and/or duration timeout, however, other period-based analytics can be used to enforce re-authentication of user sessions.	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.	3	
1.8.3	Continuous Authentication Pt 1	DoD Components applications/services utilize multiple session authentications based on security attributes and access requested. Privilege changes and associational transaction requests require additional levels of authentication such as Multi-Factor Authentication (MFA) pushes to users.	Functional	Equal	Privileged Command Execution	IAC-16.3	Mechanisms exist to ensure privilege change requests require additional levels of authentication.	10	
1.8.4	Continuous Authentication Pt 2	DoD Components continue usage of transaction-based authentication to include integration such as user patterns.	Functional	Intersects With	Continuous Authentication	IAC-13.3	Automated mechanisms exist to enable continuous re-authentication through the lifecycle of entity interactions.	8	
1.8.4	Continuous Authentication Pt 2	DoD Components continue usage of transaction-based authentication to include integration such as user patterns.	Functional	Intersects With	Attribute-Based Access Control (ABAC)	IAC-29	Mechanisms exist to enforce Attribute-Based Access Control (ABAC) for policy-driven, dynamic authorizations that supports the secure sharing of information.	8	
1.9	Integrated ICAM Platform	DoD organizations and overall enterprise employ enterprise- level identity management and public key infrastructure (PKI) systems to track user, administrator and NPE identities across the network and ensure access is limited to only those who have the need and the right to know. Organizations can verify they need and have the right to access via credential management systems, identity governance and administration tools, and an access management tool. PKI systems can be federated but must either trust a central root certificate authority (CA) and/or cross-sign standardized organizational CA's.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	8	
1.9	Integrated ICAM Platform	DoD organizations and overall enterprise employ enterprise- level identity management and public key infrastructure (PKI) systems to track user, administrator and NPE identities across the network and ensure access is limited to only those who have the need and the right to know. Organizations can verify they need and have the right to access via credential management systems, identity governance and administration tools, and an access management tool. PKI systems can be federated but must either trust a central root certificate authority (CA) and/or cross-sign standardized organizational CA's.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	8	
1.9	Integrated ICAM Platform	DoD organizations and overall enterprise employ enterprise- level identity management and public key infrastructure (PKI) systems to track user, administrator and NPE identities across the network and ensure access is limited to only those who have the need and the right to know. Organizations can verify they need and have the right to access via credential management systems, identity governance and administration tools, and an access management tool. PKI systems can be federated but must either trust a central root certificate authority (CA) and/or cross-sign standardized organizational CA's.	Functional	Intersects With	PKI-Based Authentication	IAC-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	8	
1.9.1	Enterprise PKI/IDP Pt1	The DoD Enterprise works with Components to implement Enterprise Public Key Infrastructure (PKI) solutions in a centralized and/or federated fashion. The Enterprise PKI solution utilizes a single or set of Enterprise level Root Certificate Authorities (CA) that can then be trusted by components to build Intermediate CA. Components PKI Certificated Authorities are integrated with the Enterprise PKI. An Enterprise Identity Provider (IdP) platform is implemented. The IdP solution may either be a single solution or federated set of Component IdPs with standard level of access across Components and standardized set of attributes. Components IdPs are integrated with the Enterprise IdP.	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1.9.1	Enterprise PKI/IDP Pt1	The DoD Enterprise works with Components to implement Enterprise Public Key Infrastructure (PKI) solutions in a centralized and/or federated fashion. The Enterprise PKI solution utilizes a single or set of Enterprise level Root Certificate Authorities (CA) that can then be trusted by components to build Intermediate CA. Components PKI Certificated Authorities are integrated with the Enterprise PKI. An Enterprise Identity Provider (IdP) platform is implemented. The IdP solution may either be a single solution or federated set of Component IdPs with standard level of access across Components and standardized set of attributes. Components IdPs are integrated with the Enterprise IdP.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	8	
1.9.1	Enterprise PKI/IDP Pt1	The DoD Enterprise works with Components to implement Enterprise Public Key Infrastructure (PKI) solutions in a centralized and/or federated fashion. The Enterprise PKI solution utilizes a single or set of Enterprise level Root Certificate Authorities (CA) that can then be trusted by components to build Intermediate CA. Components PKI Certificated Authorities are integrated with the Enterprise PKI. An Enterprise Identity Provider (IdP) platform is implemented. The IdP solution may either be a single solution or federated set of Component IdPs with standard level of access across Components and standardized set of attributes. Components IdPs are integrated with the Enterprise IdP.	Functional	Intersects With	PKI-Based Authentication	IAC-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	8	
1.9.2	Enterprise PKI/IDP Pt2	DoD Components enable biometric support in the Identity Provider (IdP) for mission/task-critical applications and services as appropriate. Biometric functionality is moved from Component solutions to the Enterprise. Multi-Factor Authentication (MFA) and Public Key Infrastructure (PKI) is decommissioned and migrated to the Enterprise as appropriate.	Functional	Intersects With	Biometric Authentication	IAC-10.12	Mechanisms exist to ensure biometric-based authentication satisfies organization-defined biometric quality requirements for false positives and false negatives.	5	
1.9.3	Enterprise PKI/IDP Pt3	DoD Components integrate the remaining applications/services with Biometrics functionalities. Alternative Multi-Factor Authentication (MFA) tokens can be used.	Functional	Intersects With	Biometric Authentication	IAC-10.12	Mechanisms exist to ensure biometric-based authentication satisfies organization-defined biometric quality requirements for false positives and false negatives.	5	
1.9.3	Enterprise PKI/IDP Pt3	DoD Components integrate the remaining applications/services with Biometrics functionalities. Alternative Multi-Factor Authentication (MFA) tokens can be used.	Functional	Intersects With	Alternative Multi-Factor Authentication	IAC-06.5	Mechanisms exist to enable alternative Multi-Factor Authentication (MFA) tokens when the primary MFA solution is not able to be used.	5	
2	Device	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No applicable SCF control
2.1	Device Inventory	DoD organizations establish and maintain an approved inventory list of all devices authorized to access the network and enroll all devices on the network prior to network connection. Device attributes will include technical details such as the PKI (802.1x) machine certificate, device object, patch/vulnerability status and others to enable successor activities.	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	
2.1	Device Inventory	DoD organizations establish and maintain an approved inventory list of all devices authorized to access the network and enroll all devices on the network prior to network connection. Device attributes will include technical details such as the PKI (802.1x) machine certificate, device object, patch/vulnerability status and others to enable successor activities.	Functional	Intersects With	Asset Attributes	AST-31.3	Mechanisms exist to dynamically associate asset-specific attributes to enable Attribute-Based Access Control (ABAC).	5	
2.1.1	Device Health Tool Gap Analysis	DoD Components develop an inventory of devices within the environment, and device attributes are tracked.	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	
2.1.1	Device Health Tool Gap Analysis	DoD Components develop an inventory of devices within the environment, and device attributes are tracked.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	8	
2.1.2	NPE/PKI, Device under Management	DoD Components utilize the DoD Enterprise PKI solution/service to deploy x509 certificates to all supported and managed devices. Other Non-Person Entities (NPEs) (e.g., web servers, network devices, routers, applications, etc.) that support x509 certificates are assigned them in the PKI and/or IdP systems.	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	8	
2.1.2	NPE/PKI, Device under Management	DoD Components utilize the DoD Enterprise PKI solution/service to deploy x509 certificates to all supported and managed devices. Other Non-Person Entities (NPEs) (e.g., web servers, network devices, routers, applications, etc.) that support x509 certificates are assigned them in the PKI and/or IdP systems.	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	
2.1.2	NPE/PKI, Device under Management	DoD Components utilize the DoD Enterprise PKI solution/service to deploy x509 certificates to all supported and managed devices. Other Non-Person Entities (NPEs) (e.g., web servers, network devices, routers, applications, etc.) that support x509 certificates are assigned them in the PKI and/or IdP systems.	Functional	Intersects With	PKI-Based Authentication	IAC-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	8	
2.1.3	Enterprise IDP Pt1	The DoD Enterprise Identity Provider (IdP), either using a centralized technology or federated organizational technologies, integrates Non- Person Entities (NPEs), such as devices and service accounts. Integration is tracked in the Enterprise Device Management solution when applicable as to whether it is integrated or not. NPEs not able to be integrated with the IdP are either marked for retirement or excepted using a risk-based methodical approach.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	8	
2.1.3	Enterprise IDP Pt1	The DoD Enterprise Identity Provider (IdP), either using a centralized technology or federated organizational technologies, integrates Non- Person Entities (NPEs), such as devices and service accounts. Integration is tracked in the Enterprise Device Management solution when applicable as to whether it is integrated or not. NPEs not able to be integrated with the IdP are either marked for retirement or excepted using a risk-based methodical approach.	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	
2.1.3	Enterprise IDP Pt1	The DoD Enterprise Identity Provider (IdP), either using a centralized technology or federated organizational technologies, integrates Non- Person Entities (NPEs), such as devices and service accounts. Integration is tracked in the Enterprise Device Management solution when applicable as to whether it is integrated or not. NPEs not able to be integrated with the IdP are either marked for retirement or excepted using a risk-based methodical approach.	Functional	Intersects With	Federated Credential Management	IAC-13.2	Mechanisms exist to federate credentials to allow cross-organization authentication of individuals and devices.	5	
2.1.4	Enterprise IDP Pt2	The DoD Enterprise Identity Provider (IdP), either using a centralized technology or federated organizational technologies, adds additional attributes for Non-Person Entities (NPEs) (e.g., location, usage patterns, etc.) to device profiles.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	8	
2.1.4	Enterprise IDP Pt2	The DoD Enterprise Identity Provider (IdP), either using a centralized technology or federated organizational technologies, adds additional attributes for Non-Person Entities (NPEs) (e.g., location, usage patterns, etc.) to device profiles.	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	
2.1.4	Enterprise IDP Pt2	The DoD Enterprise Identity Provider (IdP), either using a centralized technology or federated organizational technologies, adds additional attributes for Non-Person Entities (NPEs) (e.g., location, usage patterns, etc.) to device profiles.	Functional	Intersects With	Federated Credential Management	IAC-13.2	Mechanisms exist to federate credentials to allow cross-organization authentication of individuals and devices.	5	
2.2	Device Detection and Compliance	DoD organizations employ asset management systems for user devices to maintain and report on IT and Cybersecurity compliance. Managed devices (enterprise and mobile) attempting to connect to a DoD network or access a DAAS resource is detected and has its compliance status confirmed (via C2C)	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	8	
2.2	Device Detection and Compliance	DoD organizations employ asset management systems for user devices to maintain and report on IT and Cybersecurity compliance. Managed devices (enterprise and mobile) attempting to connect to a DoD network or access a DAAS resource is detected and has its compliance status confirmed (via C2C)	Functional	Intersects With	Endpoint Security Validation	NET-14.7	Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions, patch levels, etc.) prior to allowing devices to connect to organizational Technology Assets, Applications and/or Services (TAAS).	8	
2.2.1	Implement C2C/Compliance Based Network Authorization Pt1	The DoD Enterprise refines policy, standards, and requirements for Comply to Connect (C2C). Components implement and enforce compliance-based network authorization to meet ZT Target Level functionalities.	Functional	Intersects With	Endpoint Security Validation	NET-14.7	Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions, patch levels, etc.) prior to allowing devices to connect to organizational Technology Assets, Applications and/or Services (TAAS).	8	
2.2.2	Implement C2C/Compliance Based Network Authorization Pt2	DoD Components expand the deployment and usage of Comply to Connect (C2C) to all supported environments required to meet ZT advanced functionalities. C2C teams integrate their solution(s) with the Enterprise IdP and Authorization Gateways to better manage access and authorizations to resources.	Functional	Intersects With	Managed Access Control Points	NET-14.3	Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).	8	
2.2.2	Implement C2C/Compliance Based Network Authorization Pt2	DoD Components expand the deployment and usage of Comply to Connect (C2C) to all supported environments required to meet ZT advanced functionalities. C2C teams integrate their solution(s) with the Enterprise IdP and Authorization Gateways to better manage access and authorizations to resources.	Functional	Intersects With	Endpoint Security Validation	NET-14.7	Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions, patch levels, etc.) prior to allowing devices to connect to organizational Technology Assets, Applications and/or Services (TAAS).	8	
2.3	Device Authorization w/ Real Time Inspection	DoD Organizations conduct foundational and extended device tooling (NextGen AV, AppControl, File Integrity Monitoring (FIM), etc.) integration to better understand the risk posture. Organizational PKI systems are integrated to expand the existing Enterprise PKI to devices as well. Lastly Entity Activity Monitoring is also integrated to identify anomalous activities.	Functional	Subset Of	Prioritization To Address Evolving Risks & Threats	PRM-02.1	Mechanisms exist to integrate foundational cybersecurity practices with advanced technologies to maintain situation awareness of and minimize the organization's exposure to evolving risks and threats.	10	
2.3.1	Entity Activity Monitoring Pt1	Using the developed User and Device baselines, DoD Components utilize the implemented User and Entity Behavioral Activity (UEBA) solution to integrate baselines. UEBA device attributes and baselines are available to be used for device authorization.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	8	
2.3.1	Entity Activity Monitoring Pt1	Using the developed User and Device baselines, DoD Components utilize the implemented User and Entity Behavioral Activity (UEBA) solution to integrate baselines. UEBA device attributes and baselines are available to be used for device authorization.	Functional	Intersects With	Attribute-Based Access Control (ABAC)	IAC-29	Mechanisms exist to enforce Attribute-Based Access Control (ABAC) for policy-driven, dynamic authorizations that supports the secure sharing of information.	8	
2.3.2	Entity Activity Monitoring Pt2	DoD Components utilize the User and Entity Behavioral Activity (UEBA) solution with network access solutions to mandate UEBA attributes (e.g., device health, logon patterns, etc.) for accessing environments and resources.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	8	
2.3.2	Entity Activity Monitoring Pt2	DoD Components utilize the User and Entity Behavioral Activity (UEBA) solution with network access solutions to mandate UEBA attributes (e.g., device health, logon patterns, etc.) for accessing environments and resources.	Functional	Intersects With	Attribute-Based Access Control (ABAC)	IAC-29	Mechanisms exist to enforce Attribute-Based Access Control (ABAC) for policy-driven, dynamic authorizations that supports the secure sharing of information.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2.3.3	Implement Application Control & File Integrity Monitoring (FIM) Tools	DoD Components procure and implement File Integrity Monitoring (FIM) and Application control (e.g., execution deny/allow listing, containment, isolation) solutions. FIM ensures any data altered is authorized, and unauthorized changes are detected by FIM. Application containment is used to isolate any suspicious behavior or permissions to prevent any malicious lateral movement, expanding the capabilities and response of traditional executable containment. Both FIMS and application containment continues the development of the Device, Data, and Application & Workload pillars.	Functional	Intersects With	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets, Applications and/or Services (TAAS) to generate alerts for unauthorized modifications.	8	
2.3.3	Implement Application Control & File Integrity Monitoring (FIM) Tools	DoD Components procure and implement File Integrity Monitoring (FIM) and Application control (e.g., execution deny/allow listing, containment, isolation) solutions. FIM ensures any data altered is authorized, and unauthorized changes are detected by FIM. Application containment is used to isolate any suspicious behavior or permissions to prevent any malicious lateral movement, expanding the capabilities and response of traditional executable containment. Both FIMS and application containment continues the development of the Device, Data, and Application & Workload pillars.	Functional	Intersects With	Attribute-Based Access Control (ABAC)	IAC-29	Mechanisms exist to enforce Attribute-Based Access Control (ABAC) for policy-driven, dynamic authorizations that supports the secure sharing of information.	8	
2.3.4	Integrate NextGen AV Tools with C2C	DoD Component procures and implements an Endpoint Protection Platform (EPP). EPP should have the capabilities to use advanced analytics (e.g., artificial intelligence, behavioral detection, machine learning) to mitigate exploits (e.g., zero days, signatureless, fileless), provide Network Access Control, and protect against known and unknown threats. These solutions are orchestrated with the C2C or EDR solution for baseline status checks of signatures, updates, etc.	Functional	Intersects With	Endpoint Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.	8	
2.3.5	Fully Integrate Device Security stack with C2C as appropriate	DoD Components continue the deployment of Application Control to all environments and in prevention mode. File Integrity Monitoring (FIM) and Application Controls analytics are integrated into Comply to Connect (C2C) for expanded access decision making. C2C analytics are evaluated for further device/endpoint security stack data points such as UEDM and are integrated as necessary.	Functional	Intersects With	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets, Applications and/or Services (TAAS) to generate alerts for unauthorized modifications.	8	
2.3.5	Fully Integrate Device Security stack with C2C as appropriate	DoD Components continue the deployment of Application Control to all environments and in prevention mode. File Integrity Monitoring (FIM) and Application Controls analytics are integrated into Comply to Connect (C2C) for expanded access decision making. C2C analytics are evaluated for further device/endpoint security stack data points such as UEDM and are integrated as necessary.	Functional	Intersects With	Attribute-Based Access Control (ABAC)	IAC-29	Mechanisms exist to enforce Attribute-Based Access Control (ABAC) for policy-driven, dynamic authorizations that supports the secure sharing of information.	8	
2.3.5	Fully Integrate Device Security stack with C2C as appropriate	DoD Components continue the deployment of Application Control to all environments and in prevention mode. File Integrity Monitoring (FIM) and Application Controls analytics are integrated into Comply to Connect (C2C) for expanded access decision making. C2C analytics are evaluated for further device/endpoint security stack data points such as UEDM and are integrated as necessary.	Functional	Intersects With	Endpoint Security Validation	NET-14.7	Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions, patch levels, etc.) prior to allowing devices to connect to organizational Technology Assets, Applications and/or Services (TAAS).	8	
2.3.6	Enterprise PKI Pt1	The DoD Enterprise Public Key Infrastructure (PKI) is expanded to include the addition of NPE and device certificates. NPEs and devices that do not support PKI certificates are marked for retirement.	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	8	
2.3.6	Enterprise PKI Pt1	The DoD Enterprise Public Key Infrastructure (PKI) is expanded to include the addition of NPE and device certificates. NPEs and devices that do not support PKI certificates are marked for retirement.	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	
2.3.7	Enterprise PKI Pt2	DoD Components utilize certificates provisioned by the DoD Enterprise Public Key Infrastructure (PKI) for device authentication and machine to machine communications. Unsupported devices are retired and exceptions are approved and managed using a risk based methodical approach.	Functional	Intersects With	Third-Party Cryptographic Keys	CRY-09.6	Mechanisms exist to ensure customers are provided with appropriate key management guidance whenever cryptographic keys are shared.	5	
2.3.7	Enterprise PKI Pt2	DoD Components utilize certificates provisioned by the DoD Enterprise Public Key Infrastructure (PKI) for device authentication and machine to machine communications. Unsupported devices are retired and exceptions are approved and managed using a risk based methodical approach.	Functional	Intersects With	Exception Management	GOV-02.1	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	5	
2.3.7	Enterprise PKI Pt2	DoD Components utilize certificates provisioned by the DoD Enterprise Public Key Infrastructure (PKI) for device authentication and machine to machine communications. Unsupported devices are retired and exceptions are approved and managed using a risk based methodical approach.	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5	
2.4	Remote Access	DoD organizations audit existing device access processes and tooling to set a least privilege baseline. In phase 2 this access is expanded to cover basic BYOD and IOT support using the Enterprise IDP for approved applications. The final phases expand coverage to include all BYOD and IOT devices for services using the approved set of device attributes.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	8	
2.4	Remote Access	DoD organizations audit existing device access processes and tooling to set a least privilege baseline. In phase 2 this access is expanded to cover basic BYOD and IOT support using the Enterprise IDP for approved applications. The final phases expand coverage to include all BYOD and IOT devices for services using the approved set of device attributes.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	8	
2.4	Remote Access	DoD organizations audit existing device access processes and tooling to set a least privilege baseline. In phase 2 this access is expanded to cover basic BYOD and IOT support using the Enterprise IDP for approved applications. The final phases expand coverage to include all BYOD and IOT devices for services using the approved set of device attributes.	Functional	Intersects With	Endpoint Security Validation	NET-14.7	Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions, patch levels, etc.) prior to allowing devices to connect to organizational Technology Assets, Applications and/or Services (TAAS).	5	
2.4.1	Deny Device by Default Policy	DoD Enterprise sets standards and requirements for overall policy, with Components tailoring to specific environmentse and mission requirements. DoD Components will block access from all unmanaged remote and local devices to resources. Managed compliant devices are provided risk-based, methodical access following ZT Target Level concepts.	Functional	Intersects With	Managed Access Control Points	NET-14.3	Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).	8	
2.4.1	Deny Device by Default Policy	DoD Enterprise sets standards and requirements for overall policy, with Components tailoring to specific environmentse and mission requirements. DoD Components will block access from all unmanaged remote and local devices to resources. Managed compliant devices are provided risk-based, methodical access following ZT Target Level concepts.	Functional	Intersects With	Endpoint Security Validation	NET-14.7	Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions, patch levels, etc.) prior to allowing devices to connect to organizational Technology Assets, Applications and/or Services (TAAS).	8	
2.4.2	Managed and Limited BYOD & IOT Support	DoD Components utilize Enterprise Device Management Solution to ensure that managed Bring Your Own Device (BYOD) and Internet of Things (IoT) devices are fully integrated with Enterprise IdP. Enabling user and device-based authorization is supported. Device access requires dynamic access policies and the practice of least privilege.	Functional	Intersects With	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	8	
2.4.2	Managed and Limited BYOD & IOT Support	DoD Components utilize Enterprise Device Management Solution to ensure that managed Bring Your Own Device (BYOD) and Internet of Things (IoT) devices are fully integrated with Enterprise IdP. Enabling user and device-based authorization is supported. Device access requires dynamic access policies and the practice of least privilege.	Functional	Intersects With	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	5	
2.4.2	Managed and Limited BYOD & IOT Support	DoD Components utilize Enterprise Device Management Solution to ensure that managed Bring Your Own Device (BYOD) and Internet of Things (IoT) devices are fully integrated with Enterprise IdP. Enabling user and device-based authorization is supported. Device access requires dynamic access policies and the practice of least privilege.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	
2.4.2	Managed and Limited BYOD & IOT Support	DoD Components utilize Enterprise Device Management Solution to ensure that managed Bring Your Own Device (BYOD) and Internet of Things (IoT) devices are fully integrated with Enterprise IdP. Enabling user and device-based authorization is supported. Device access requires dynamic access policies and the practice of least privilege.	Functional	Intersects With	Attribute-Based Access Control (ABAC)	IAC-29	Mechanisms exist to enforce Attribute-Based Access Control (ABAC) for policy-driven, dynamic authorizations that supports the secure sharing of information.	8	
2.4.3	Managed and Full BYOD & IOT Support Pt1	DoD Components utilize Unified Endpoint and Device Management (UEDM) and similar solutions to enable access for managed and approved devices to Mission and Operational Critical services/applications using dynamic access policies. BYOD and Internet of Things (IoT) devices are required to meet standard baseline checks before authorization.	Functional	Intersects With	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	8	
2.4.3	Managed and Full BYOD & IOT Support Pt1	DoD Components utilize Unified Endpoint and Device Management (UEDM) and similar solutions to enable access for managed and approved devices to Mission and Operational Critical services/applications using dynamic access policies. BYOD and Internet of Things (IoT) devices are required to meet standard baseline checks before authorization.	Functional	Intersects With	Endpoint Security Validation	NET-14.7	Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions, patch levels, etc.) prior to allowing devices to connect to organizational Technology Assets, Applications and/or Services (TAAS).	8	
2.4.4	Managed and Full BYOD & IOT Support Pt2	DoD Components utilize Unified Endpoint and Device Management (UEDM) and similar solutions to grant authorized managed devices access to all services and applications where possible. Unmanaged devices, upon meeting device checks and standard baselines, are granted access to services and applications following a risk-based authorization approach.	Functional	Intersects With	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	8	
2.4.4	Managed and Full BYOD & IOT Support Pt2	DoD Components utilize Unified Endpoint and Device Management (UEDM) and similar solutions to grant authorized managed devices access to all services and applications where possible. Unmanaged devices, upon meeting device checks and standard baselines, are granted access to services and applications following a risk-based authorization approach.	Functional	Intersects With	Endpoint Security Validation	NET-14.7	Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions, patch levels, etc.) prior to allowing devices to connect to organizational Technology Assets, Applications and/or Services (TAAS).	8	
2.5	Partially & Fully Automated Asset, Vulnerability and Patch Management	DoD organizations establish processes to automatically test and deploy vendor patches for connected devices; hybrid patch management (both human and automated) is employed.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
2.5	Partially & Fully Automated Asset, Vulnerability and Patch Management	DoD organizations establish processes to automatically test and deploy vendor patches for connected devices; hybrid patch management (both human and automated) is employed.	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	
2.5	Partially & Fully Automated Asset, Vulnerability and Patch Management	DoD organizations establish processes to automatically test and deploy vendor patches for connected devices; hybrid patch management (both human and automated) is employed.	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	
2.5.1	Implement Asset, Vulnerability and Patch Management Tools	DoD Components implement solution(s) for managing asset/device configurations, vulnerabilities, and patches. Using minimum compliance standards (e.g., STIGs, C2C, UEM etc.), teams can confirm or deny managed device compliance. As part of the procurement and implementation process for solutions, APIs or other programmatic interfaces will be in scope for future levels of automation and integration.	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	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2.5.1	Implement Asset, Vulnerability and Patch Management Tools	DoD Components implement solution(s) for managing asset/device configurations, vulnerabilities, and patches. Using minimum compliance standards (e.g., STIGs, C2C, UEM etc.), teams can confirm or deny managed device compliance. As part of the procurement and implementation process for solutions, APIs or other programmatic interfaces will be in scope for future levels of automation and integration.	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.	8	
2.5.1	Implement Asset, Vulnerability and Patch Management Tools	DoD Components implement solution(s) for managing asset/device configurations, vulnerabilities, and patches. Using minimum compliance standards (e.g., STIGs, C2C, UEM etc.), teams can confirm or deny managed device compliance. As part of the procurement and implementation process for solutions, APIs or other programmatic interfaces will be in scope for future levels of automation and integration.	Functional	Intersects With	Endpoint Security Validation	NET-14.7	Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions, patch levels, etc.) prior to allowing devices to connect to organizational Technology Assets, Applications and/or Services (TAAS).	8	
2.5.1	Implement Asset, Vulnerability and Patch Management Tools	DoD Components implement solution(s) for managing asset/device configurations, vulnerabilities, and patches. Using minimum compliance standards (e.g., STIGs, C2C, UEM etc.), teams can confirm or deny managed device compliance. As part of the procurement and implementation process for solutions, APIs or other programmatic interfaces will be in scope for future levels of automation and integration.	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.	8	
2.5.1	Implement Asset, Vulnerability and Patch Management Tools	DoD Components implement solution(s) for managing asset/device configurations, vulnerabilities, and patches. Using minimum compliance standards (e.g., STIGs, C2C, UEM etc.), teams can confirm or deny managed device compliance. As part of the procurement and implementation process for solutions, APIs or other programmatic interfaces will be in scope for future levels of automation and integration.	Functional	Intersects With	Endpoint Security Validation	NET-14.7	Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions, patch levels, etc.) prior to allowing devices to connect to organizational Technology Assets, Applications and/or Services (TAAS).	8	
2.6	Unified Endpoint Management (UEM) & Mobile Device Management (MDM)	DoD organizations establish a centralized UEM solution that provides the choices of agent and/or agentless management of computer and mobile devices to a single console regardless of device location. DoD-issued devices can be remotely managed and security policies are enforced.	Functional	Equal	Unified Endpoint Device Management (UEDM)	END-01.1	Mechanisms exist to utilize a centralized Unified Endpoint Device Management (UEDM) solution that provides agent and/or agentless management of endpoint devices regardless of device location.	10	
2.6.1	Implement UEDM or equivalent Tools	DoD Components will work closely with the "Implement Asset, Vulnerability, and Patch Management Tools" activity to procure a implement and Unified Endpoint Device Management (UEDM) solution ensuring that requirements are integrated with the procurement process. Once a solution is procured the UEDM team(s) ensure that critical ZT Target Level functionalities such as minimum compliance, asset management, and API support are in place.	Functional	Subset Of	Unified Endpoint Device Management (UEDM)	END-01.1	Mechanisms exist to utilize a centralized Unified Endpoint Device Management (UEDM) solution that provides agent and/or agentless management of endpoint devices regardless of device location.	10	
2.6.2	Enterprise Device Management Pt1	DoD Enterprise sets standards and policies for Enterprise Device Management (EDM). DoD Components migrate the manual device inventory to an automated approach using an EDM solution. Approved devices are able to be managed regardless of location. Devices part of critical services are managed by the EDM solution supporting automation.	Functional	Subset Of	Unified Endpoint Device Management (UEDM)	END-01.1	Mechanisms exist to utilize a centralized Unified Endpoint Device Management (UEDM) solution that provides agent and/or agentless management of endpoint devices regardless of device location.	10	
2.6.3	Enterprise Device Management Pt2	DoD Components migrate the remaining devices to Enterprise Device Management (EDM) solution. EDM solution is integrated with risk and compliance solutions as appropriate.	Functional	Subset Of	Unified Endpoint Device Management (UEDM)	END-01.1	Mechanisms exist to utilize a centralized Unified Endpoint Device Management (UEDM) solution that provides agent and/or agentless management of endpoint devices regardless of device location.	10	
2.7	Endpoint & Extended Detection & Response (EDR & XDR)	DoD organizations use endpoint detection and response (EDR) tooling to monitor, detect, and remediate malicious activity on endpoints. Expanding the capability to include XDR tooling allows organizations to account for activity beyond the endpoints such as cloud and network as well.	Functional	Intersects With	Unified Endpoint Device Management (UEDM)	END-01.1	Mechanisms exist to utilize a centralized Unified Endpoint Device Management (UEDM) solution that provides agent and/or agentless management of endpoint devices regardless of device location.	8	
2.7	Endpoint & Extended Detection & Response (EDR & XDR)	DoD organizations use endpoint detection and response (EDR) tooling to monitor, detect, and remediate malicious activity on endpoints. Expanding the capability to include XDR tooling allows organizations to account for activity beyond the endpoints such as cloud and network as well.	Functional	Intersects With	Endpoint Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.	8	
2.7.1	Implement Endpoint Detection & Response (EDR) Tools and Integrate with C2C	DoD Components procure and implement Endpoint Detection and Response (EDR) solution(s) within environments. EDR is protecting, monitoring, and responding to malicious and anomalous activities enabling ZT Target Level functionality and is sending data to the Comply to Connect (C2C) solution for expanded device and user checks.	Functional	Equal	Endpoint Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.	10	
2.7.2	Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt1	DoD Components procure and implement Extended Detection & Response (XDR) solution(s). Integration points with cross pillar capabilities (network, cloud services, applications) are identified and prioritized based on risk. XDR is aligned with C2C program. XDR capabilities either supplement or replace EDR implementations. Analysis and correlation capabilities are sent from the XDR solution stack to the SIEM.	Functional	Intersects With	Unified Endpoint Device Management (UEDM)	END-01.1	Mechanisms exist to utilize a centralized Unified Endpoint Device Management (UEDM) solution that provides agent and/or agentless management of endpoint devices regardless of device location.	8	
2.7.2	Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt1	DoD Components procure and implement Extended Detection & Response (XDR) solution(s). Integration points with cross pillar capabilities (network, cloud services, applications) are identified and prioritized based on risk. XDR is aligned with C2C program. XDR capabilities either supplement or replace EDR implementations. Analysis and correlation capabilities are sent from the XDR solution stack to the SIEM.	Functional	Intersects With	Endpoint Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.	8	
2.7.2	Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt1	DoD Components procure and implement Extended Detection & Response (XDR) solution(s). Integration points with cross pillar capabilities (network, cloud services, applications) are identified and prioritized based on risk. XDR is aligned with C2C program. XDR capabilities either supplement or replace EDR implementations. Analysis and correlation capabilities are sent from the XDR solution stack to the SIEM.	Functional	Intersects With	Extended Detection & Response (XDR)	END-06.8	Mechanisms exist to implement Extended Detection & Response (XDR) technologies to correlate data and respond to threats across multiple security layers, including:(1) Endpoints;(2) On-premises networks;(3) Cloud-based networks;(4) Electronic communications;(5) Applications; and(6) Services.	8	
2.7.2	Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt1	DoD Components procure and implement Extended Detection & Response (XDR) solution(s). Integration points with cross pillar capabilities (network, cloud services, applications) are identified and prioritized based on risk. XDR is aligned with C2C program. XDR capabilities either supplement or replace EDR implementations. Analysis and correlation capabilities are sent from the XDR solution stack to the SIEM.	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	3	
2.7.3	Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt2	Extended Detection & Response (XDR) solution stack completes identification of integration points expanding coverage to the fullest amount possible. Exceptions are tracked and managed using a risk- based approach for continued operation. Extended analytics enabling ZT Advanced Level functionalities are integrated into the SIEM and other appropriate solutions.	Functional	Intersects With	Extended Detection & Response (XDR)	END-06.8	Mechanisms exist to implement Extended Detection & Response (XDR) technologies to correlate data and respond to threats across multiple security layers, including:(1) Endpoints;(2) On-premises networks;(3) Cloud-based networks;(4) Electronic communications;(5) Applications; and(6) Services.	8	
2.7.3	Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt2	Extended Detection & Response (XDR) solution stack completes identification of integration points expanding coverage to the fullest amount possible. Exceptions are tracked and managed using a risk- based approach for continued operation. Extended analytics enabling ZT Advanced Level functionalities are integrated into the SIEM and other appropriate solutions.	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	5	
2.7.3	Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt2	Extended Detection & Response (XDR) solution stack completes identification of integration points expanding coverage to the fullest amount possible. Exceptions are tracked and managed using a risk- based approach for continued operation. Extended analytics enabling ZT Advanced Level functionalities are integrated into the SIEM and other appropriate solutions.	Functional	Intersects With	Exception Management	GOV-02.1	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	5	
3	Applications and Workloads	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No applicable SCF control
3.1	Application Inventory	System owners ensure that all applications and application components are identified and inventoried; only applications and application components that have been authorized by the appropriate authorizing official/CISO/CIO shall be utilized within the system owner's purview	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	
3.1.1	Application/Code Identification	DoD Components create an inventory of approved applications and code being used, including open-source, commercial, and in-house developed software. Each Component will track the supportability (i.e., active, legacy, etc.) hosted location (i.e., cloud, on-premises, hybrid, etc.) and record important data (i.e., name, version, team responsible, licensing and support, mapped dependencies).	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	
3.1.1	Application/Code Identification	DoD Components create an inventory of approved applications and code being used, including open-source, commercial, and in-house developed software. Each Component will track the supportability (i.e., active, legacy, etc.) hosted location (i.e., cloud, on-premises, hybrid, etc.) and record important data (i.e., name, version, team responsible, licensing and support, mapped dependencies).	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-04.2	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	5	
3.2	Secure Software Development & Integration	Foundational software and application security processes and infrastructure are established following Zero Trust principles and best practices. Controls such as code review, runtime protection, secure API gateways, container and serverless security are integrated and automated.	Functional	Intersects With	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	8	
3.2	Secure Software Development & Integration	Foundational software and application security processes and infrastructure are established following Zero Trust principles and best practices. Controls such as code review, runtime protection, secure API gateways, container and serverless security are integrated and automated.	Functional	Subset Of	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	
3.2.1	Build DevSecOps Software Factory Pt1	The DoD Enterprise provide best practices for modern DevSecOps processes and CI/CD pipelines. The concepts are applied in a standardized technology stack across DoD Components able to meet future Application Security requirements, including requirements gathering, design, development, testing and deployment.	Functional	Subset Of	DevSecOps	TDA-01.4	Mechanisms exist to integrate security, compliance and resilience into Development, Security and Operations (DevSecOps) to prioritize secure practices throughout the Software Development Lifecycle (SDLC).	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
3.2.2	Build DevSecOps Software Factory Pt2	DoD Components use their approved CI/CD pipelines to develop most new applications. Any exceptions will follow a standardized approval process to be allowed to develop in a legacy fashion. DevSecOps processes are also used to develop all new applications and update existing applications. Continual validation functions are integrated into the CI/CD pipelines and DevSecOps processes and integrated with existing applications.	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	
3.2.2	Build DevSecOps Software Factory Pt2	DoD Components use their approved CI/CD pipelines to develop most new applications. Any exceptions will follow a standardized approval process to be allowed to develop in a legacy fashion. DevSecOps processes are also used to develop all new applications and update existing applications. Continual validation functions are integrated into the CI/CD pipelines and DevSecOps processes and integrated with existing applications.	Functional	Intersects With	DevSecOps	TDA-01.4	Mechanisms exist to integrate security, compliance and resilience into Development, Security and Operations (DevSecOps) to prioritize secure practices throughout the Software Development Lifecycle (SDLC).	8	
3.2.3	Automate Application Security & Code Remediation Pt1	A standardized approach to application security including code remediation is implemented across the DoD enterprise. Part one (1) of this activity includes the integration of securing API gateways (i.e., API management, WAF, continuous API testing, distributed enforcement not just perimeter) with applications utilizing API or similar calls. Code reviews are conducted in a methodical approach, and standardized protections for containers and their infrastructure are in place. Additionally, any serverless functions where the 3rd party manages the infrastructure, such as Platform as a Service, utilize adequate serverless security monitoring and response functions. Code reviews, container and serverless security functions are integrated into the CI/CD and/or DevSecOps process, as appropriate.	Functional	Subset Of	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and(3) Document the results.	10	
3.2.4	Automate Application Security & Code Remediation Pt2	DoD Components modernize approaches to delivering internally developed and managed applications following best practice approaches such as a Microservices architecture. These approaches will enhance security and resilience by enabling rapid code updates within individual microservices to address vulnerabilities. Further enhance application security by integrating runtime security functions for containers where applicable, automating vulnerable library updates, and automating CI/CD approvals during the release process.	Functional	Subset Of	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	
3.3	Software Risk Management	DoD organizations establish software/application risk management program. Foundational controls include Bill of Materials risk management, Supplier Risk Management, approved repositories and update channels, and vulnerability management program. Additional controls include Continual validation within the CI/CD pipelines and vulnerability maturation with external sources.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
3.3	Software Risk Management	DoD organizations establish software/application risk management program. Foundational controls include Bill of Materials risk management, Supplier Risk Management, approved repositories and update channels, and vulnerability management program. Additional controls include Continual validation within the CI/CD pipelines and vulnerability maturation with external sources.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	8	
3.3	Software Risk Management	DoD organizations establish software/application risk management program. Foundational controls include Bill of Materials risk management, Supplier Risk Management, approved repositories and update channels, and vulnerability management program. Additional controls include Continual validation within the CI/CD pipelines and vulnerability maturation with external sources.	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-04.2	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	5	
3.3	Software Risk Management	DoD organizations establish software/application risk management program. Foundational controls include Bill of Materials risk management, Supplier Risk Management, approved repositories and update channels, and vulnerability management program. Additional controls include Continual validation within the CI/CD pipelines and vulnerability maturation with external sources.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and(3) Document the results.	5	
3.3.1	Approved Binaries/Code	The DoD Enterprise uses best practices to manage approved binaries and code in a methodical approac, including supplier sourcing risk management, approved repository usage, Software Bill of Materials (SBOM), supply chain risk management, and industry-standard vulnerability management.	Functional	Intersects With	Access to Program Source Code	TDA-20	Mechanisms exist to limit privileges to change software resident within software libraries.	8	
3.3.1	Approved Binaries/Code	The DoD Enterprise uses best practices to manage approved binaries and code in a methodical approac, including supplier sourcing risk management, approved repository usage, Software Bill of Materials (SBOM), supply chain risk management, and industry-standard vulnerability management.	Functional	Intersects With	Approved Code	TDA-20.4	Mechanisms exist to govern the approval of binaries and code for production use.	8	
3.3.2	Vulnerability Management Program Pt1	The DoD Enterprise collaborates with Components to establish and manage a comprehensive Vulnerability Management program. The program, at a minimum, encompasses the tracking and management of public vulnerabilities based on DoD applications and services. Each Component is responsible for establishing a vulnerability management team comprised of key stakeholders. This team convenes to discuss and manage vulnerabilities in accordance with established Enterprise policy and standards.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
3.3.3	Vulnerability Management Program Pt2	Processes are established at the DoD Enterprise level for managing the disclosure of vulnerabilities in DoD maintained and operated services, both publicly and privately accessible. DoD Components expand the vulnerability management program to track and manage closed vulnerability repositories such as DIB-VDP, CERT, and others.	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	
3.3.4	Continual Validation	DoD Components implement a continuous validation approach for application development, where security is constantly assessed throughout the development, integration, and deployment. Validation includes security principles when planning and designing, security testing (to include code reviews), incident response, and SIEM alerting/logging. These principles are integrated and continuously executed with the CI/CD pipeline. Applications developed outside of CI/CD process should still adhere to continuous validation in an ad hoc/manual manner.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and(3) Document the results.	8	
3.4	Resource Authorization & Integration	DoD establishes a standardized resource authorization gateway for authorizations via the CI/CD pipelines in a risk approach that reviews the User, Device and Data security posture. Authorizations utilize a programmatic (e.g., Software Defined) approach in a live/production environment. Attributes are enriched utilizing other pillar activities and the API and Authorization gateway. Approved enterprise APIs are micro- segmented using authorizations.	Functional	Intersects With	API Gateway	TDA-23	Mechanisms exist to implement an Application Programming Interface (API) Gateway, or similar technology, to serve as a controlled entry point that manages interactions between client-facing requests and backend services.	8	
3.4.1	Resource Authorization Pt1	The DoD Enterprise standardizes policy enforcement approaches (e.g., Software Defined Perimeter) with the Components. At a minimum, the access and authorization gateways will be integrated with identities and devices once authentication is achieved. Components deploy approved resource authorization gateways and enable them for external facing applications and services. Additional applications for migration and applications unable to be migrated are identified for exception or decommission.	Functional	Intersects With	API Gateway	CLD-04.1	Mechanisms exist to implement an Application Programming Interface (API) Gateway, or similar technology, to serve as a controlled entry point that manages interactions between client-facing requests and backend services.	8	
3.4.2	Resource Authorization Pt2	Policy enforcements and decisions are used for all possible applications and services. Application unable to utilize gateways are either decommissioned or accepted using a risk-based methodical approach. Authorizations are further integrated with the CI/CD pipeline for automated decision making.	Functional	Intersects With	Policy Decision Point (PDP)	NET-04.7	Automated mechanisms exist to evaluate access requests against established criteria to dynamically and uniformly enforce access rights and permissions.	8	
3.4.3	SDC Resource Authorization Pt1	The DoD Enterprise establishes best practices for code-based compute management (i.e., Software Defined Compute(SDC)). Using risk-based approaches, baselines are created using the approved set of code libraires and packages. DoD Components work with the approved code/binaries activities to ensure that applications are identified which can and cannot support the approach. Applications that can support a modern software-based configuration and management approaches are identified, and transitioning begins. Applications that cannot follow software-based configuration and management approaches are identified and allowed through exception using a methodical approach.	Functional	Intersects With	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	5	
3.4.4	SDC Resource Authorization Pt2	Components use approved and validated code/binaries via the Software Bill of Materials (SBOM) process to ensure that applications that can and cannot support the approach are identified. Applications which can support modern Software-Based Configuration and Management (SBCM) approaches are identified and transitioned. Applications that support SBCM have been transitioned to a production/live environment and are in normal operations. Applications which cannot SBCM are identified and allowed through exception using a risk-based approach.	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-04.2	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	5	
3.4.5	Enrich Attributes for Resource Authorization Pt1	Initial attributes from various sources, such as User and Entity Activity Monitoring (UEAM), micro-segmentation services, Data Loss Prevention (DLP), and Digital Rights Management (DRM) tools are integrated with the Resource Authorization technology system and policies. Any additional attributes for later integration are identified and planned. Attributes are used to create basic risk posture of users, NPEs and devices allowing for authorization decisions based on the evaluated risk.	Functional	Subset Of	Behavioral Baselining	THR-11	Automated mechanisms exist to establish behavioral baselines that capture information about user and entity behavior to enable dynamic threat discovery.	10	
3.4.6	Enrich Attributes for Resource Authorization Pt2	Extended identified attributes are integrated with the resource authorization technology and policy. Confidence scoring system is introduced for identified attributes to create a more advanced method of authorization decision making supporting.	Functional	Intersects With	Asset Attributes	AST-31.3	Mechanisms exist to dynamically associate asset-specific attributes to enable Attribute-Based Access Control (ABAC).	5	
3.4.6	Enrich Attributes for Resource Authorization Pt2	Extended identified attributes are integrated with the resource authorization technology and policy. Confidence scoring system is introduced for identified attributes to create a more advanced method of authorization decision making supporting.	Functional	Intersects With	Behavioral Baselining	THR-11	Automated mechanisms exist to establish behavioral baselines that capture information about user and entity behavior to enable dynamic threat discovery.	5	
3.4.7	REST API Micro-Segments	Using the DoD Enterprise approved API gateway(s), application calls are micro-segmented, only allowing authenticated and authorized access to specific destinations (e.g., microservices). When possible, API micro- segmentation consoles are integrated and aware of other micro- segmentation consoles such as Software Defined Perimeter (SDP)controllers and/or Software Defined Networking (SDN) consoles.	Functional	Intersects With	Microsegmentation	NET-06.6	Automated mechanisms exist to enable microsegmentation, either physically or virtually, to divide the network according to application and data workflows communications needs.	5	
3.4.7	REST API Micro-Segments	Using the DoD Enterprise approved API gateway(s), application calls are micro-segmented, only allowing authenticated and authorized access to specific destinations (e.g., microservices). When possible, API micro- segmentation consoles are integrated and aware of other micro- segmentation consoles such as Software Defined Perimeter (SDP)controllers and/or Software Defined Networking (SDN) consoles.	Functional	Intersects With	Software Defined Networking (SDN)	NET-06.7	Automated mechanisms exist to enable dynamic, policy-driven network segmentation, access controls and traffic management with a Software Defined Networking (SDN) architecture.	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
3.5	Continuous Monitoring and Ongoing Authorizations	DoD organizations employ automated tools and processes to continuously monitor applications and assess their authorization to operate.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
3.5.1	Continuous Authorization to Operate (cATO) Pt1	DoD Components utilize automation solutions within the environment to standardize the monitoring of controls and offer the capability to identify deviations. Where appropriate, monitoring and testing is integrated with DevSecOps processes.	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	
3.5.1	Continuous Authorization to Operate (cATO) Pt1	DoD Components utilize automation solutions within the environment to standardize the monitoring of controls and offer the capability to identify deviations. Where appropriate, monitoring and testing is integrated with DevSecOps processes.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	8	
3.5.1	Continuous Authorization to Operate (cATO) Pt1	DoD Components utilize automation solutions within the environment to standardize the monitoring of controls and offer the capability to identify deviations. Where appropriate, monitoring and testing is integrated with DevSecOps processes.	Functional	Intersects With	Integration of Scanning & Other Monitoring Information	MON-02.3	Automated mechanisms exist to integrate the analysis of audit records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further enhance the ability to identify inappropriate or unusual activity.	8	
3.5.2	Continuous Authorization to Operate (cATO) Pt2	DoD Components fully automate control derivation, testing and monitoring processes. Deviations are automatically tested and resolved using existing cross pillar automation infrastructure. Dashboards are used to monitor the status of authorizations; analytics are integrated with the responsible authorizing officials.	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	
3.5.2	Continuous Authorization to Operate (cATO) Pt2	DoD Components fully automate control derivation, testing and monitoring processes. Deviations are automatically tested and resolved using existing cross pillar automation infrastructure. Dashboards are used to monitor the status of authorizations; analytics are integrated with the responsible authorizing officials.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	8	
3.5.2	Continuous Authorization to Operate (cATO) Pt2	DoD Components fully automate control derivation, testing and monitoring processes. Deviations are automatically tested and resolved using existing cross pillar automation infrastructure. Dashboards are used to monitor the status of authorizations; analytics are integrated with the responsible authorizing officials.	Functional	Intersects With	Integration of Scanning & Other Monitoring Information	MON-02.3	Automated mechanisms exist to integrate the analysis of audit records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further enhance the ability to identify inappropriate or unusual activity.	8	
4	Data	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No applicable SCF control
4.1	Data Catalog Risk Alignment	Data owners ensure that data is identified and inventoried and any changes to the data landscape are automatically detected and included within the catalog. The data landscape must then be reviewed to identify potential risks related to data loss, attack, or any other unauthorized alteration and/or access.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	8	
4.1	Data Catalog Risk Alignment	Data owners ensure that data is identified and inventoried and any changes to the data landscape are automatically detected and included within the catalog. The data landscape must then be reviewed to identify potential risks related to data loss, attack, or any other unauthorized alteration and/or access.	Functional	Intersects With	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	5	
4.1.1	Data Analysis	The DoD Enterprise will develop algorithm(s) for components to map data for tagging and labeling, and establish the governing body for oversight. Data at a Component level should be categorized and analyzed by an overseeing governing body.	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.	8	
4.1.1	Data Analysis	The DoD Enterprise will develop algorithm(s) for components to map data for tagging and labeling, and establish the governing body for oversight. Data at a Component level should be categorized and analyzed by an overseeing governing body.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that:(1) Contain sufficient detail to assess the security of the network's architecture;(2) Reflect the current architecture of the network environment; and(3) Document all sensitive/regulated data flows.	3	
4.2	DoD Enterprise Data Governance	DoD establishes enterprise data labeling/tagging and DAAS access control/sharing policies (e.g., SDS policy) that are enforceable. Developed enterprise standards ensure an appropriate level of interoperability between DoD Organizations.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	8	
4.2	DoD Enterprise Data Governance	DoD establishes enterprise data labeling/tagging and DAAS access control/sharing policies (e.g., SDS policy) that are enforceable. Developed enterprise standards ensure an appropriate level of interoperability between DoD Organizations.	Functional	Intersects With	Data Tagging	PRI-11	Mechanisms exist to issue data modeling guidelines to support tagging of sensitive/regulated data.	5	
4.2.1	Define Data Tagging Standards	Data tagging standard for identifying ZT labels must be defined. The DoD Enterprise works with Components to establish data tagging and classification standards based on industry best practices. Classifications are agreed upon and implemented in processes. Tags are identified as manual and automated for future activities.	Functional	No Relationship	N/A	N/A	N/A	N/A	No applicable SCF control
4.2.2	Interoperability Standards	The DoD Enterprise, collaborating with Components, develops interoperability standards methods including mandatory Data Rights Management (DRM) overlays and Protection mechanisms with necessary technologies to enable ZT Target Level functionality.	Functional	No Relationship	N/A	N/A	N/A	N/A	No applicable SCF control
4.2.3	Develop Software Defined Storage (SDS) Policy	The DoD enterprise will work with Components to determine if software define storage (SDS) is in use. DoD Components develop policy and standards based on industry best practices, and evaluate current data storage strategy and technology for implementation of SDS.Components assess their existing data storage strategies and technologies to determine the suitability for implementing SDS. If deemed appropriate, the identified storage technologies are considered for SDS implementation.	Functional	No Relationship	N/A	N/A	N/A	N/A	No applicable SCF control
4.3	Data Labeling and Tagging	Data owners label and tag data in compliance with DoD enterprise governance on labeling/tagging policy. As phases advance automation is used to meet scaling demands and provide better accuracy.	Functional	Intersects With	Data Tagging	PRI-11	Mechanisms exist to issue data modeling guidelines to support tagging of sensitive/regulated data.	5	
4.3.1	Implement Data Tagging & Classification Tools	DoD Components implement a solution to create new rules, modify existing rules, delete existing rules, check for rule collision, rule deviation, or compound rule inconsistency, and testing of collective rule sets for an outcome. Tools must be adaptable to advanced analytic techniques.	Functional	No Relationship	N/A	N/A	N/A	N/A	No applicable SCF control
4.3.2	Manual Data Tagging Pt1	Components map DoD Enterprise ZT tags to local labeling to meet minimum essential metadata criteria for compliance.	Functional	Intersects With	Data Tagging	PRI-11	Mechanisms exist to issue data modeling guidelines to support tagging of sensitive/regulated data.	5	
4.3.3	Manual Data Tagging Pt2	DoD Component specific data level attributes are integrated into the manual data tagging process. DoD Enterprise and Components collaborate to decide which attributes are required to meet ZT Advanced Level functionality. Data level attributes for ZT Advanced Level functionality is standardized across the Enterprise and incorporated.	Functional	Intersects With	Cybersecurity & Data Protection Attributes	DCH-05	Mechanisms exist to bind cybersecurity and data protection attributes to information as it is stored, transmitted and processed.	5	
4.3.3	Manual Data Tagging Pt2	DoD Component specific data level attributes are integrated into the manual data tagging process. DoD Enterprise and Components collaborate to decide which attributes are required to meet ZT Advanced Level functionality. Data level attributes for ZT Advanced Level functionality is standardized across the Enterprise and incorporated.	Functional	Intersects With	Data Tagging	PRI-11	Mechanisms exist to issue data modeling guidelines to support tagging of sensitive/regulated data.	5	
4.3.4	Automated Data Tagging & Support Pt1	DoD Components use Data Loss Prevention (DLP), Data Rights Management (DRM), and/or protection solutions to conduct scanning of data repositories. Standardized tags are applied to supported data repositories and data types. Unsupported data repositories and types are identified.	Functional	Intersects With	Data Rights Management (DRM)	DCH-27	Mechanisms exist to utilize Data Rights Management (DRM), or similar technologies, to protect Intellectual Property (IP) rights by preventing the unauthorized distribution and/or modification of sensitive IP.	5	
4.3.4	Automated Data Tagging & Support Pt1	DoD Components use Data Loss Prevention (DLP), Data Rights Management (DRM), and/or protection solutions to conduct scanning of data repositories. Standardized tags are applied to supported data repositories and data types. Unsupported data repositories and types are identified.	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
4.3.5	Automated Data Tagging & Support Pt2	Remaining supported data repositories have basic and extended data tags applied using Machine Learning (ML) and Artificial Intelligence (AI). Extended data tags are applied to existing repositories. Unsupported data repositories and data types are evaluated for decommissioning using a risk-based methodical approach. Approved exceptions utilize manual data tagging approaches with data owners and/or custodians to manage tagging.	Functional	Intersects With	Cybersecurity & Data Protection Attributes	DCH-05	Mechanisms exist to bind cybersecurity and data protection attributes to information as it is stored, transmitted and processed.	3	
4.4	Data Monitoring and Sensing	Data owners will capture active metadata that includes information about the access, sharing, transformation, and use of their data assets. Data Loss Prevention (DLP) and Data Rights Management (DRM) enforcement point analysis is conducted to determine where tooling will be deployed. Data outside of DLP and DRM scope such as File Shares and Databases is actively monitored for anomalous and malicious activity using alternative tooling.	Functional	Intersects With	Metadata	NET-04.5	Mechanisms exist to enforce information flow controls based on metadata.	5	
4.4.1	DLP Enforcement Point Logging and Analysis	DoD Components identify business rules for managing data loss prevention (DLP) enforcement points, such as specific services and user endpoints. Using the established DoD Enterprise cybersecurity incident response standard, DoD Components ensure the appropriate level of detail of data is captured. Additionally, protection, detection, and response use cases are developed to better outline solution coverage.	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
4.4.2	DRM Enforcement Point Logging and Analysis	DoD Components identify business rules for managing the accepted use of the assets managing Data Rights Management (DRM) enforcement points, such as specific services and user endpoints. Using the established DoD Enterprise cybersecurity incident response standard, DoD Components ensure the appropriate detail of data is captured. Additionally, protection, detection, and response use cases are developed to better outline solution coverage.	Functional	Intersects With	Data Rights Management (DRM)	DCH-27	Mechanisms exist to utilize Data Rights Management (DRM), or similar technologies, to protect Intellectual Property (IP) rights by preventing the unauthorized distribution and/or modification of sensitive IP.	5	
4.4.2	DRM Enforcement Point Logging and Analysis	DoD Components identify business rules for managing the accepted use of the assets managing Data Rights Management (DRM) enforcement points, such as specific services and user endpoints. Using the established DoD Enterprise cybersecurity incident response standard, DoD Components ensure the appropriate detail of data is captured. Additionally, protection, detection, and response use cases are developed to better outline solution coverage.	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	
4.4.3	File Activity Monitoring Pt1	DoD Components utilize File Monitoring tools to monitor the most critical data classification levels in applications, services, and repositories. Analytics from monitoring is fed into the SIEM with basic data attributes to accomplish ZT Target Level functionality.	Functional	Intersects With	File Activity Monitoring (FAM)	MON-18	Automated mechanisms exist to monitor sensitive/regulated data in Technology Assets, Applications and/or Services (TAAS) and data repositories.	8	
4.4.3	File Activity Monitoring Pt1	DoD Components utilize File Monitoring tools to monitor the most critical data classification levels in applications, services, and repositories. Analytics from monitoring is fed into the SIEM with basic data attributes to accomplish ZT Target Level functionality.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	8	
4.4.4	File Activity Monitoring Pt2	DoD Components utilize File Monitoring tools to monitor all regulatory protected data (e.g., CUI, PII, PHI, etc.) in applications, services, and repositories. Extended integration is used to send data to appropriate inter/intra-pillar solutions such as Data Loss Prevention, Data Rights Management/Protection and User & Entity Behavior Analytics.	Functional	Intersects With	File Activity Monitoring (FAM)	MON-18	Automated mechanisms exist to monitor sensitive/regulated data in Technology Assets, Applications and/or Services (TAAS) and data repositories.	8	
4.4.4	File Activity Monitoring Pt2	DoD Components utilize File Monitoring tools to monitor all regulatory protected data (e.g., CUI, PII, PHI, etc.) in applications, services, and repositories. Extended integration is used to send data to appropriate inter/intra-pillar solutions such as Data Loss Prevention, Data Rights Management/Protection and User & Entity Behavior Analytics.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	8	

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
4.4.5	Database Activity Monitoring	DoD Components procure, implement, and utilize database monitoring solutions to monitor all databases containing regulated data types (e.g., CUI, PII, PHI, etc.). Logs and analytics from the database monitoring solution are provided to the SIEM for monitoring and response. Analytics are utilized in cross pillar activities such as "Enterprise Security Profile Pt 1, Pt 2" and "Real Time Access Decisions" to better direct decision making.	Functional	Intersects With	File Activity Monitoring (FAM)	MON-18	Automated mechanisms exist to monitor sensitive/regulated data in Technology Assets, Applications and/or Services (TAAS) and data repositories.	8	
4.4.5	Database Activity Monitoring	DoD Components procure, implement, and utilize database monitoring solutions to monitor all databases containing regulated data types (e.g., CUI, PII, PHI, etc.). Logs and analytics from the database monitoring solution are provided to the SIEM for monitoring and response. Analytics are utilized in cross pillar activities such as "Enterprise Security Profile Pt 1, Pt 2" and "Real Time Access Decisions" to better direct decision making.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	8	
4.4.6	Comprehensive Data Activity Monitoring	DoD Components expand monitoring of data repositories including databases as appropriate, based on a methodical risk-based approach. Additional data attributes to meet the ZT Advanced Level functionalities are integrated into the analytics for additional integrations.	Functional	Intersects With	Database Management System (DBMS)	AST-28.1	Mechanisms exist to implement and maintain Database Management Systems (DBMSs), where applicable.	3	
4.4.6	Comprehensive Data Activity Monitoring	DoD Components expand monitoring of data repositories including databases as appropriate, based on a methodical risk-based approach. Additional data attributes to meet the ZT Advanced Level functionalities are integrated into the analytics for additional integrations.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	8	
4.5	Data Encryption & Rights Management	DoD organizations establish and implement a strategy for encrypting data at rest and in transit using Data Rights Management (DRM) tooling. The DRM solution utilizes data tags to determine protection and lastly integrates with ML and AI to automate protection.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	8	
4.5	Data Encryption & Rights Management	DoD organizations establish and implement a strategy for encrypting data at rest and in transit using Data Rights Management (DRM) tooling. The DRM solution utilizes data tags to determine protection and lastly integrates with ML and AI to automate protection.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
4.5	Data Encryption & Rights Management	DoD organizations establish and implement a strategy for encrypting data at rest and in transit using Data Rights Management (DRM) tooling. The DRM solution utilizes data tags to determine protection and lastly integrates with ML and AI to automate protection.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
4.5	Data Encryption & Rights Management	DoD organizations establish and implement a strategy for encrypting data at rest and in transit using Data Rights Management (DRM) tooling. The DRM solution utilizes data tags to determine protection and lastly integrates with ML and AI to automate protection.	Functional	Intersects With	Data Rights Management (DRM)	DCH-27	Mechanisms exist to utilize Data Rights Management (DRM), or similar technologies, to protect Intellectual Property (IP) rights by preventing the unauthorized distribution and/or modification of sensitive IP.	5	
4.5.1	Implement DRM and Protection Tools Pt1	DoD Components procure and implement DRM and Protection solution(s) as needed, following the DoD Enterprise standard and requirements. Newly implement DRM and protection solution(s) are applied with high-risk data objects.	Functional	Intersects With	Data Rights Management (DRM)	DCH-27	Mechanisms exist to utilize Data Rights Management (DRM), or similar technologies, to protect Intellectual Property (IP) rights by preventing the unauthorized distribution and/or modification of sensitive IP.	8	
4.5.2	Implement DRM and Protection Tools Pt2	DRM and protection coverage is expanded to cover all required data objects. Protection mechanisms are automatically managed to meet best practices (e.g., FIPS). Extended data protection attributes are implemented based on the environment classification.	Functional	Intersects With	Data Rights Management (DRM)	DCH-27	Mechanisms exist to utilize Data Rights Management (DRM), or similar technologies, to protect Intellectual Property (IP) rights by preventing the unauthorized distribution and/or modification of sensitive IP.	5	
4.5.3	DRM Enforcement via Data Tags and Analytics Pt1	DoD Enterprise provides a standard for data access control and protections. Components establish data rights management (DRM) and protection solutions that are used with data tags defined by the data producer. High-risk data objects are identified and monitored with protect and response actions enabled. Data at rest is encrypted and protected (e.g., hardware/object/disk encryption, access control) in repositories.	Functional	Intersects With	Data Rights Management (DRM)	DCH-27	Mechanisms exist to utilize Data Rights Management (DRM), or similar technologies, to protect Intellectual Property (IP) rights by preventing the unauthorized distribution and/or modification of sensitive IP.	5	
4.5.4	DRM Enforcement via Data Tags and Analytics Pt2	Extended data repositories are protected with DRM and protection solutions. DoD Components implement extended data tags applicable to Components versus Enterprise. Data is encrypted in extended repositories using additional tags.	Functional	Intersects With	Data Rights Management (DRM)	DCH-27	Mechanisms exist to utilize Data Rights Management (DRM), or similar technologies, to protect Intellectual Property (IP) rights by preventing the unauthorized distribution and/or modification of sensitive IP.	5	
4.5.5	DRM Enforcement via Data Tags and Analytics Pt3	DRM and protection solutions integrate with AI and ML tooling for encryption, rights management, and protection functions.	Functional	Intersects With	Data Rights Management (DRM)	DCH-27	Mechanisms exist to utilize Data Rights Management (DRM), or similar technologies, to protect Intellectual Property (IP) rights by preventing the unauthorized distribution and/or modification of sensitive IP.	5	
4.6	Data Loss Prevention (DLP)	DoD organizations utilize the identified enforcement points to deploy approved DLP tools and integrate tagged data attributes with DLP. Initially the DLP solution is put into a "monitor-only" mode to limit business impact and later using analytics is put into a "prevent" mode. Extended data tag attributes are used to feed the DLP solution and lastly integrate with ML and AI.	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	8	
4.6.1	Implement Enforcement Points	Data loss prevention (DLP) is aligned to and strengthened by Data Privacy and Protection (DPP). Then through attribution, attributes can be injected that address where data is coming from, its movement across ZT control boundaries, and the invocation of protection measures (e.g., encryption, obfuscation, etc.). Data loss prevention (DLP) solution is deployed to the in-scope enforcement points. It is recommended to start with "monitor-only" and/or "learning" mode limiting impact. Collaboration with cyber functions should occur with respect to any observed data loss activity.	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	8	
4.6.2	DLP Enforcement via Data Tags and Analytics Pt1	Data loss prevention (DLP) solution is updated from monitor only mode to prevention mode. Zero Trust tagging incorporates indicators to facilitate DLP through cooperative cyber enforcement.	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	8	
4.6.3	DLP Enforcement via Data Tags and Analytics Pt2	Data Loss Prevention (DLP) solution is updated to include extended data tags based on parallel automation activities.	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
4.6.4	DLP Enforcement via Data Tags and Analytics Pt3	Data Loss Prevention (DLP) solution is integrated with automated data tagging techniques, to include any missing enforcement points and tags.	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
4.7	Data Access Control	DoD organizations ensure appropriate access to and use of data based on the data and user/NPE/device properties. Software Defined Storage (SDS) is utilized to scale manage permissions to DAAS. Lastly the SDS solution(s) is integrated with DRM tooling improving protections.	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.	8	
4.7	Data Access Control	DoD organizations ensure appropriate access to and use of data based on the data and user/NPE/device properties. Software Defined Storage (SDS) is utilized to scale manage permissions to DAAS. Lastly the SDS solution(s) is integrated with DRM tooling improving protections.	Functional	Intersects With	Software Defined Storage (SDS)	CLD-15	Automated mechanisms exist to utilize Software Defined Storage (SDS) to scale access management permissions to Technology Assets, Applications, Services and/or Data (TAASD).	8	
4.7	Data Access Control	DoD organizations ensure appropriate access to and use of data based on the data and user/NPE/device properties. Software Defined Storage (SDS) is utilized to scale manage permissions to DAAS. Lastly the SDS solution(s) is integrated with DRM tooling improving protections.	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	8	
4.7	Data Access Control	DoD organizations ensure appropriate access to and use of data based on the data and user/NPE/device properties. Software Defined Storage (SDS) is utilized to scale manage permissions to DAAS. Lastly the SDS solution(s) is integrated with DRM tooling improving protections.	Functional	Intersects With	Data Rights Management (DRM)	DCH-27	Mechanisms exist to utilize Data Rights Management (DRM), or similar technologies, to protect Intellectual Property (IP) rights by preventing the unauthorized distribution and/or modification of sensitive IP.	5	
4.7.1	Integrate DAAS Access w/SDS Policy Pt1	Governance mechanisms ensure that component DAAS policy is sufficient for Zero Trust outcomes as established by the SDS policy, if deemed appropriate as established in "4.2.3 Develop Software Defined Storage (SDS) Policy".	Functional	Intersects With	Software Defined Storage (SDS)	CLD-15	Automated mechanisms exist to utilize Software Defined Storage (SDS) to scale access management permissions to Technology Assets, Applications, Services and/or Data (TAASD).	8	
4.7.2	Integrate DAAS Access w/SDS Policy Pt2	DoD Components implement the DAAS policy in an automated fashion.	Functional	Intersects With	Software Defined Storage (SDS)	CLD-15	Automated mechanisms exist to utilize Software Defined Storage (SDS) to scale access management permissions to Technology Assets, Applications, Services and/or Data (TAASD).	8	
4.7.3	Integrate DAAS Access w/SDS Policy Pt3	Newly implemented SDS technology and/or functionalities are integrated with the DAAS policy in a risk-based fashion. A phased approach is taken during implementation to measure results and adjust accordingly.	Functional	Intersects With	Software Defined Storage (SDS)	CLD-15	Automated mechanisms exist to utilize Software Defined Storage (SDS) to scale access management permissions to Technology Assets, Applications, Services and/or Data (TAASD).	8	
4.7.4	Integrate Solution(s) and Policy with Enterprise IDP Pt1	DoD Components integrate attributes associated with access control and data location, and establishes a means for interoperability across DLP, DRM, and storage infrastructure solutions with Enterprise IdP.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	5	
4.7.4	Integrate Solution(s) and Policy with Enterprise IDP Pt1	DoD Components integrate attributes associated with access control and data location, and establishes a means for interoperability across DLP, DRM, and storage infrastructure solutions with Enterprise IdP.	Functional	Intersects With	Software Defined Storage (SDS)	CLD-15	Automated mechanisms exist to utilize Software Defined Storage (SDS) to scale access management permissions to Technology Assets, Applications, Services and/or Data (TAASD).	5	
4.7.4	Integrate Solution(s) and Policy with Enterprise IDP Pt1	DoD Components integrate attributes associated with access control and data location, and establishes a means for interoperability across DLP, DRM, and storage infrastructure solutions with Enterprise IdP.	Functional	Intersects With	Data Rights Management (DRM)	DCH-27	Mechanisms exist to utilize Data Rights Management (DRM), or similar technologies, to protect Intellectual Property (IP) rights by preventing the unauthorized distribution and/or modification of sensitive IP.	5	
4.7.4	Integrate Solution(s) and Policy with Enterprise IDP Pt1	DoD Components integrate attributes associated with access control and data location, and establishes a means for interoperability across DLP, DRM, and storage infrastructure solutions with Enterprise IdP.	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
4.7.5	Integrate Solution(s) and Policy with Enterprise IDP Pt2	Newly implemented SDS technology and/or functionalities are integrated with the Enterprise Identity Provider (IdP) following the integration plan. Identity attributes required to meet ZT Target Level functionalities are required for integration.	Functional	Intersects With	Software Defined Storage (SDS)	CLD-15	Automated mechanisms exist to utilize Software Defined Storage (SDS) to scale access management permissions to Technology Assets, Applications, Services and/or Data (TAASD).	8	
4.7.6	Implement SDS Tool and/or integrate with DRM Tool Pt1	Depending on the need for a Software Defined Storage (SDS) tool, a new solution is implemented, or an existing solution is identified, meeting the functionality requirements to be integrated with DLP, DRM, and ML solutions.	Functional	Intersects With	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	5	
4.7.6	Implement SDS Tool and/or integrate with DRM Tool Pt1	Depending on the need for a Software Defined Storage (SDS) tool, a new solution is implemented, or an existing solution is identified, meeting the functionality requirements to be integrated with DLP, DRM, and ML solutions.	Functional	Intersects With	Software Defined Storage (SDS)	CLD-15	Automated mechanisms exist to utilize Software Defined Storage (SDS) to scale access management permissions to Technology Assets, Applications, Services and/or Data (TAASD).	5	
4.7.6	Implement SDS Tool and/or integrate with DRM Tool Pt1	Depending on the need for a Software Defined Storage (SDS) tool, a new solution is implemented, or an existing solution is identified, meeting the functionality requirements to be integrated with DLP, DRM, and ML solutions.	Functional	Intersects With	Data Rights Management (DRM)	DCH-27	Mechanisms exist to utilize Data Rights Management (DRM), or similar technologies, to protect Intellectual Property (IP) rights by preventing the unauthorized distribution and/or modification of sensitive IP.	5	
4.7.6	Implement SDS Tool and/or integrate with DRM Tool Pt1	Depending on the need for a Software Defined Storage (SDS) tool, a new solution is implemented, or an existing solution is identified, meeting the functionality requirements to be integrated with DLP, DRM, and ML solutions.	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
4.7.7	Implement SDS Tool and/or integrate with DRM Tool Pt2	DoD Components configure the SDS functionality and/or solution to be integrated with the underlying DLP and DRM infrastructure as appropriate. Lower-level integrations enable more effective protection and response.	Functional	Intersects With	Software Defined Storage (SDS)	CLD-15	Automated mechanisms exist to utilize Software Defined Storage (SDS) to scale access management permissions to Technology Assets, Applications, Services and/or Data (TAASD).	5	
4.7.7	Implement SDS Tool and/or integrate with DRM Tool Pt2	DoD Components configure the SDS functionality and/or solution to be integrated with the underlying DLP and DRM infrastructure as appropriate. Lower-level integrations enable more effective protection and response.	Functional	Intersects With	Data Rights Management (DRM)	DCH-27	Mechanisms exist to utilize Data Rights Management (DRM), or similar technologies, to protect Intellectual Property (IP) rights by preventing the unauthorized distribution and/or modification of sensitive IP.	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
4.7.7	Implement SDS Tool and/or integrate with DRM Tool Pt2	DoD Components configure the SDS functionality and/or solution to be integrated with the underlying DLP and DRM infrastructure as appropriate. Lower-level integrations enable more effective protection and response.	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
5	Network and Environment	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No applicable SCF control
5.1	Data Flow Mapping	DoD organizations reconcile data flows by gathering, mapping, and visualizing network traffic data flows and patterns to ensure authorized access and protection for network and DAAS resources specifically tagging programmatic (e.g., API) access when possible.	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.	8	
5.1	Data Flow Mapping	DoD organizations reconcile data flows by gathering, mapping, and visualizing network traffic data flows and patterns to ensure authorized access and protection for network and DAAS resources specifically tagging programmatic (e.g., API) access when possible.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that:(1) Contain sufficient detail to assess the security of the network's architecture;(2) Reflect the current architecture of the network environment; and(3) Document all sensitive/regulated data flows.	8	
5.1.1	Define Granular Control Access Rules & Policies Pt1	The DoD Enterprise working with the Components creates granular network access rules and policies. Associated Concept of Operations (ConOps) are developed in alignment with access policies as well ensure future supportability. Once agreed upon, DoD Components will implement these access policies into existing network technologies (e.g., Next Generation Firewalls, Intrusion Prevention Systems, etc.) to improve initial risk levels and ensure future interoperability.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
5.1.1	Define Granular Control Access Rules & Policies Pt1	The DoD Enterprise working with the Components creates granular network access rules and policies. Associated Concept of Operations (ConOps) are developed in alignment with access policies as well ensure future supportability. Once agreed upon, DoD Components will implement these access policies into existing network technologies (e.g., Next Generation Firewalls, Intrusion Prevention Systems, etc.) to improve initial risk levels and ensure future interoperability.	Functional	Intersects With	Zero Trust Architecture (ZTA)	NET-01.1	Mechanisms exist to treat all users and devices as potential threats and prevent access to data and resources until the users can be properly authenticated and their access authorized.	8	
5.1.2	Define Granular Control Access Rules & Policies Pt2	DoD Components utilize data tagging and classification standards to develop data filters for API access to the SDN or alternative networking approach. API Decision Points are formalized within the SDN or alternative network architecture and implemented with non- mission/task critical applications and services.	Functional	Intersects With	Asset Attributes	AST-31.3	Mechanisms exist to dynamically associate asset-specific attributes to enable Attribute-Based Access Control (ABAC).	8	
5.1.2	Define Granular Control Access Rules & Policies Pt2	DoD Components utilize data tagging and classification standards to develop data filters for API access to the SDN or alternative networking approach. API Decision Points are formalized within the SDN or alternative network architecture and implemented with non- mission/task critical applications and services.	Functional	Intersects With	Cybersecurity & Data Protection Attributes	DCH-05	Mechanisms exist to bind cybersecurity and data protection attributes to information as it is stored, transmitted and processed.	8	
5.1.2	Define Granular Control Access Rules & Policies Pt2	DoD Components utilize data tagging and classification standards to develop data filters for API access to the SDN or alternative networking approach. API Decision Points are formalized within the SDN or alternative network architecture and implemented with non- mission/task critical applications and services.	Functional	Intersects With	Policy Decision Point (PDP)	NET-04.7	Automated mechanisms exist to evaluate access requests against established criteria to dynamically and uniformly enforce access rights and permissions.	5	
5.2	Software Defined Networking (SDN)	DoD organizations define API decision points and implement SDN programmable infrastructure to separate the control and data planes and centrally manage and control the elements in the data plane. Integrations are conducted with decision points and segmentation gateway to accomplish the plane separation. Analytics are then integrated to real time decision making for access to resources.	Functional	Intersects With	Policy Decision Point (PDP)	NET-04.7	Automated mechanisms exist to evaluate access requests against established criteria to dynamically and uniformly enforce access rights and permissions.	8	
5.2.1	Define SDN APIs	The DoD Enterprise works with Components to define the necessary APIs and other programmatic interfaces that enable Software Defined Networking (SDN) or alternative networking approach functionalities. These APIs will enable authentication decision point, application delivery control proxy and ssegmentation gateways automation.	Functional	Intersects With	Software Defined Networking (SDN)	NET-06.7	Automated mechanisms exist to enable dynamic, policy-driven network segmentation, access controls and traffic management with a Software Defined Networking (SDN) architecture.	8	
5.2.2	Implement SDN Programable Infrastructure	Following the API standards, requirements, and SDN API functionalities, DoD Components will implement SoftwareDefined Networking (SDN) or alternative networking approach infrastructure to enable automation tasks. Segmentation gateways and authentication decision points are integrated into the SDN or alternative networking approach infrastructure along with output logging into a standardized repository (e.g., SIEM, Log Analytics) for monitoring and alerting.	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	5	
5.2.2	Implement SDN Programable Infrastructure	Following the API standards, requirements, and SDN API functionalities, DoD Components will implement SoftwareDefined Networking (SDN) or alternative networking approach infrastructure to enable automation tasks. Segmentation gateways and authentication decision points are integrated into the SDN or alternative networking approach infrastructure along with output logging into a standardized repository (e.g., SIEM, Log Analytics) for monitoring and alerting.	Functional	Intersects With	Policy Decision Point (PDP)	NET-04.7	Automated mechanisms exist to evaluate access requests against established criteria to dynamically and uniformly enforce access rights and permissions.	8	
5.2.2	Implement SDN Programable Infrastructure	Following the API standards, requirements, and SDN API functionalities, DoD Components will implement SoftwareDefined Networking (SDN) or alternative networking approach infrastructure to enable automation tasks. Segmentation gateways and authentication decision points are integrated into the SDN or alternative networking approach infrastructure along with output logging into a standardized repository (e.g., SIEM, Log Analytics) for monitoring and alerting.	Functional	Intersects With	Software Defined Networking (SDN)	NET-06.7	Automated mechanisms exist to enable dynamic, policy-driven network segmentation, access controls and traffic management with a Software Defined Networking (SDN) architecture.	8	
5.2.3	Segment Flows into Control, Management, and Data Planes	Network infrastructure and flows are segmented either physically or logically into separate and distinct control, management, and data planes. Segmentation using IPv6/VLAN approaches is implemented to better organize traffic across data planes. Analytics and NetFlow from the updated infrastructure is automatically fed into Operations Centers and analytics tools.	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.	8	
5.2.4	Network Asset Discovery & Optimization	DoD Components automate network asset discovery through the SDN infrastructure, limiting access to devices based on risk-based methodical approaches. Optimization is conducted based on the SDN analytics to improve overall performance along with providing approved access to resources.	Functional	Intersects With	Automated Network Asset Discovery	AST-32	Mechanisms exist to automate network asset discovery through Software Defined Networking (SDN), or similar technologies, that analyzes network traffic to:(1) Identify;(2) Document; and(3) Track devices.	8	
5.2.5	Real-Time Access Decisions	SDN infrastructure utilizes cross pillar data sources such as User Activity Monitoring (UAM), Entity Activity Monitoring (EAM), Enterprise security profiles, and more, for real-time access decisions. Machine Learning (ML) is used to assist decision making based on advanced network analytics (i.e., full packet capture, etc.). Policies are consistently implemented across the Enterprise using unified access standards.	Functional	Intersects With	Real-Time Access Decisions	IAC-29.1	Automated mechanisms exist to utilize Machine Learning (ML) to make real-time access decisions based on advanced network analytics that leverages enterprise-wide data sources.	8	
5.3	Macro Segmentation	DoD organizations establish network boundaries and provide security against networked assets located within an environment by validating the device, user, or NPE on each attempt of accessing a remote resource prior to connection.	Functional	Equal	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	10	
5.3.1	Datacenter Macro segmentation	DoD Components implement service-based architectures to restrict lateral movement between public and private components of a solutions architecture. Proxy and/or enforcement checks are integrated with the SDN or alternative networking approach solution(s) based on device attributes and behavior.	Functional	Intersects With	Microsegmentation	NET-06.6	Automated mechanisms exist to enable microsegmentation, either physically or virtually, to divide the network according to application and data workflows communications needs.	8	
5.3.2	B/C/P/S Macro segmentation	DoD Components implement mission/organization-based macro- segmentation using logical network zones that limit lateral movement. Proxy and/or enforcement checks are integrated with the SDN or alternative networking approach solution(s) based on device attributes and behavior.	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	
5.4	Micro Segmentation	DoD organizations define and document network segmentation based on identity and / or application access in their virtualized and/or cloud environments. Automation is used to apply policy changes through programmatic (e.g., API) approaches. Lastly where possible organizations will utilize host-level process micro segmentation.	Functional	Intersects With	Microsegmentation	NET-06.6	Automated mechanisms exist to enable microsegmentation, either physically or virtually, to divide the network according to application and data workflows communications needs.	5	
5.4.1	Implement Micro segmentation	DoD Components implement micro-segmentation infrastructure into SDN or alternative networking approach environment, enabling basic segmentation of service components (e.g., web, app, DB), ports, and protocols. Basic automation is accepted for policy changes, including API decision making. Virtual hosting environments implement micro- segmentation at the host/container-level.	Functional	Intersects With	Microsegmentation	NET-06.6	Automated mechanisms exist to enable microsegmentation, either physically or virtually, to divide the network according to application and data workflows communications needs.	5	
5.4.2	Application & Device Micro segmentation	DoD Components utilize Software Defined Networking (SDN) or alternative networking approach solution(s) to establish infrastructure meeting the ZT Target Level functionalities - i.e., logical network zones; Role, Attribute, and Condition-Based Access Control for Users and Devices, Privileged Access Management (PAM) services for network resources, and policy-based control on API access.	Functional	Intersects With	Microsegmentation	NET-06.6	Automated mechanisms exist to enable microsegmentation, either physically or virtually, to divide the network according to application and data workflows communications needs.	8	
5.4.2	Application & Device Micro segmentation	DoD Components utilize Software Defined Networking (SDN) or alternative networking approach solution(s) to establish infrastructure meeting the ZT Target Level functionalities - i.e., logical network zones; Role, Attribute, and Condition-Based Access Control for Users and Devices, Privileged Access Management (PAM) services for network resources, and policy-based control on API access.	Functional	Intersects With	Software Defined Networking (SDN)	NET-06.7	Automated mechanisms exist to enable dynamic, policy-driven network segmentation, access controls and traffic management with a Software Defined Networking (SDN) architecture.	8	
5.4.3	Process Micro segmentation	DoD Components utilize existing micro-segmentation and SDN automation infrastructure enabling process micro-segmentation. Host- level processes are segmented based on security policies and access is granted using real-time access decision making.	Functional	Intersects With	Microsegmentation	NET-06.6	Automated mechanisms exist to enable microsegmentation, either physically or virtually, to divide the network according to application and data workflows communications needs.	8	
5.4.4	Protect Data In Transit	Based on the data flow mappings and monitoring standards provided by DoD Enterprise, policies are enabled by DoD Components to mandate protection of data in transit. Common use cases, such as Coalition Information Sharing, sharing across system boundaries and protection across architectural components, are included in protection policies.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	5	
6	Automation and Orchestration	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No applicable SCF control
6.1	Policy Decision Point (PDP) & Policy Orchestration	DoD organizations initially collect and document all rule based policies to orchestrate across the security stack for effective automation; DAAS access procedures and policies will be defined, implemented, and updated. Organizations mature this capability by establishing PDPs and PEPs (including the Next Generation Firewall) to make DAAS resource determinations and enable, monitor, and terminate connections between a user/device and DAAS resources according to predefined policy.	Functional	Intersects With	Policy Decision Point (PDP)	NET-04.7	Automated mechanisms exist to evaluate access requests against established criteria to dynamically and uniformly enforce access rights and permissions.	8	
6.1.1	Policy Inventory & Development	The DoD Enterprise works with Components to catalog and inventory existing cybersecurity policies and standards. Policies are updated and created in cross-pillar activities as needed to meet critical ZT Target Level functionality.	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.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
6.1.2	Organization Access Profile	DoD Components develop access profile rules for mission/task and non-mission/task DAAS access using the data from the User, Data, Network & Environment, and Device pillars. The DoD Enterprise works with the Components to develop an Enterprise security profile rules using the existing Component security profiles to create a common access approach to DAAS. A phased approach can be used by Components to limit risk to mission/task critical DAAS access once the security profile(s) are created.	Functional	Intersects With	Access Profile Rules	IAC-29.2	Mechanisms exist to develop access profile rules for sensitive/regulated Technology Assets, Applications, Services and/or Data (TAASD) access based on User, Data, Network, Environment & Device attributes.	8	
6.1.3	Enterprise Security Profile Pt1	Enterprise security profile rules covers the User, Data, Network & Environment, and Device pillars initially. Existing Component security profile rules are integrated for non-mission/task DAAS access following an iterative approach to tuning access.	Functional	Intersects With	Real-Time Access Decisions	IAC-29.1	Automated mechanisms exist to utilize Machine Learning (ML) to make real-time access decisions based on advanced network analytics that leverages enterprise-wide data sources.	8	
6.1.3	Enterprise Security Profile Pt1	Enterprise security profile rules covers the User, Data, Network & Environment, and Device pillars initially. Existing Component security profile rules are integrated for non-mission/task DAAS access following an iterative approach to tuning access.	Functional	Intersects With	Access Profile Rules	IAC-29.2	Mechanisms exist to develop access profile rules for sensitive/regulated Technology Assets, Applications, Services and/or Data (TAASD) access based on User, Data, Network, Environment & Device attributes.	8	
6.1.4	Enterprise Security Profile Pt2	The minimum number of Enterprise security profile(s) exist that grant access to the widest range of DAAS within the DoD Compontents. Mission/task Component profiles are integrated with the Enterprise security profile(s) and exceptions are managed in a risk-based methodical approach.	Functional	Intersects With	Access Profile Rules	IAC-29.2	Mechanisms exist to develop access profile rules for sensitive/regulated Technology Assets, Applications, Services and/or Data (TAASD) access based on User, Data, Network, Environment & Device attributes.	5	
6.2	Critical Process Automation	DoD organizations employ automation methods, such as RPA, to address repetitive, predictable tasks for critical functions such as data enrichment, security controls, and incident response workflows according to system security engineering principles.	Functional	Intersects With	Robotic Process Automation (RPA)	AAT-32	Mechanisms exist to implement Robotic Process Automation (RPA) to improve efficiency, accuracy and speed for high-volume, repetitive and rules-based business processes.	8	
6.2.1	Task Automation Analysis	DoD Components identify and enumerate all task activities that can be executed both manually and in an automated fashion. Task activities are organized into automated and manual categories. Manual activities are analyzed for retirement.	Functional	Intersects With	Business Process Task Enumeration	AAT-32.1	Mechanisms exist to identify and enumerate business process task activities that can be executed both manually and in an automated fashion.	8	
6.2.2	Enterprise Integration & Workflow Provisioning Pt1	The DoD Enterprise establishes baseline integration and interoperability within the Security Orchestration, Automation, and Response (SOAR) solution required to enable ZTA Target Level functionality, where actionable and relevant information resides. DoD Components identify instrument, integration, and interoperability points and prioritization per the Enterprise baseline. The necessary integrations in User, Device, Application & Workload, Network & Environment, and Device pillars to automate IR functions are completed.	Functional	Intersects With	Robotic Process Automation (RPA)	AAT-32	Mechanisms exist to implement Robotic Process Automation (RPA) to improve efficiency, accuracy and speed for high-volume, repetitive and rules-based business processes.	5	
6.2.3	Enterprise Integration & Workflow Provisioning Pt2	DoD Components integrate remaining services to meet baseline requirements and ZT Advanced Level functionality requirements. Service provisioning is integrated and automated into workflows, where required, meeting ZT Target Level functionalities.	Functional	Intersects With	Zero Trust Architecture (ZTA)	NET-01.1	Mechanisms exist to treat all users and devices as potential threats and prevent access to data and resources until the users can be properly authenticated and their access authorized.	5	
6.3	Machine Learning	DoD organizations employ ML to execute (and enhance execution of) critical functions such as incident response, anomaly detection, user baselining, and data tagging.	Functional	Intersects With	Robotic Process Automation (RPA)	AAT-32	Mechanisms exist to implement Robotic Process Automation (RPA) to improve efficiency, accuracy and speed for high-volume, repetitive and rules-based business processes.	8	
6.3.1	Implement Data Tagging & Classification ML Tools	DoD Components utilize existing Data Tagging and Classification standards and requirements to integrate Machine Learning (ML) solution(s)/capability as needed. ML solution(s) is implemented by Components, and existing tagged and classified data repositories are used to establish baselines. ML solution(s) applies data tags in a supervised approach to continually improve analysis.	Functional	Intersects With	Robotic Process Automation (RPA)	AAT-32	Mechanisms exist to implement Robotic Process Automation (RPA) to improve efficiency, accuracy and speed for high-volume, repetitive and rules-based business processes.	5	
6.4	Artificial Intelligence	DoD organizations employ AI to execute (and enhance execution of) critical functions - particularly risk and access determinations and environmental analysis.	Functional	Subset Of	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	10	
6.4	Artificial Intelligence	DoD organizations employ AI to execute (and enhance execution of) critical functions - particularly risk and access determinations and environmental analysis.	Functional	Intersects With	Robotic Process Automation (RPA)	AAT-32	Mechanisms exist to implement Robotic Process Automation (RPA) to improve efficiency, accuracy and speed for high-volume, repetitive and rules-based business processes.	8	
6.4.1	Implement AI automation tools	DoD Components identify areas of improvement based on existing Machine Learning (ML) techniques for Artificial Intelligence (AI). AI solutions are identified, procured, and implemented using the identified areas as requirements.	Functional	Subset Of	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	10	
6.4.2	AI Driven by Analytics decides A&O modifications	DoD Components, utilizing existing Machine Learning (ML) functions, implement and use AI technology, such as neural networks, to drive automation and orchestration decisions. Decision making is moved to AI as much as possible, freeing up human staff for other efforts. Utilizing historical patterns, AI will make anticipatory changes in the environment to better reduce risk.	Functional	Subset Of	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	10	
6.4.2	AI Driven by Analytics decides A&O modifications	DoD Components, utilizing existing Machine Learning (ML) functions, implement and use AI technology, such as neural networks, to drive automation and orchestration decisions. Decision making is moved to AI as much as possible, freeing up human staff for other efforts. Utilizing historical patterns, AI will make anticipatory changes in the environment to better reduce risk.	Functional	Intersects With	Robotic Process Automation (RPA)	AAT-32	Mechanisms exist to implement Robotic Process Automation (RPA) to improve efficiency, accuracy and speed for high-volume, repetitive and rules-based business processes.	8	
6.5	Security Orchestration, Automation & Response (SOAR)	DoD organizations achieve initial operational capability of security technologies to orchestrate and automate policies (e.g., PEPs and PDPs) and rulesets to improve security operations, threat and vulnerability management, and security incident response by ingesting alert data, triggering playbooks for automated response and remediation.	Functional	Equal	Security Orchestration, Automation, and Response (SOAR)	OPS-06	Mechanisms exist to utilize Security Orchestration, Automation and Response (SOAR) tools to define, prioritize and automate the response to security incidents.	10	
6.5.1	Response Automation Analysis	DoD Components identify and enumerate all response activities that are executed both manually and in an automated fashion. Response activities are organized into automated and manual categories.	Functional	Subset Of	Business Process Task Enumeration	AAT-32.1	Mechanisms exist to identify and enumerate business process task activities that can be executed both manually and in an automated fashion.	10	
6.5.2	Implement SOAR Tools	DoD Enterprise, working with Components, develops a standard set of requirements for Security Orchestration, Automation, and Response (SOAR) tooling to enable ZT Target Level functionallity. DoD Components use approved requirements to procure and implement a SOAR solutions. Iinfrastructure integrations for future SOAR functionality is completed.	Functional	Intersects With	Security Orchestration, Automation, and Response (SOAR)	OPS-06	Mechanisms exist to utilize Security Orchestration, Automation and Response (SOAR) tools to define, prioritize and automate the response to security incidents.	8	
6.5.3	Implement Playbooks	DoD Components review all existing playbooks to identify for future automation. Existing manual and automated processes missing playbooks have playbooks developed. Playbooks are prioritized for automation to be integrated with the "Automated Workflows" activities covering critical processes. Manual processes without playbooks are authorized using a risk-based methodical approach.	Functional	Intersects With	Secure Practices Guidelines	OPS-05	Mechanisms exist to provide guidelines and recommendations for the secure use of Technology Assets, Applications and/or Services (TAAS) to assist in the configuration, installation and use of the product and/or service.	8	
6.6	API Standardization	DoD establishes and enforces enterprise-wide programmatic interface (e.g., API) standards; all non-compliant APIs are identified and replaced.	Functional	Intersects With	Application Programming Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application Programming Interfaces (APIs).	8	
6.6.1	Tool Compliance Analysis	Automation and Orchestration tooling and solutions are analyzed for compliance and capabilities based on the DoD Enterprise API machine- readable patterns and protocols.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
6.6.1	Tool Compliance Analysis	Automation and Orchestration tooling and solutions are analyzed for compliance and capabilities based on the DoD Enterprise API machine- readable patterns and protocols.	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	
6.6.2	Standardized API Calls & Schemas Pt1	The DoD Enterprise works with components to establish an API standard (or equivalent automated interchange mechanism), which at least outlines the approved patterns and protocols. DoD Components identify existing APIs and update to the standard.	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	
6.6.2	Standardized API Calls & Schemas Pt1	The DoD Enterprise works with components to establish an API standard (or equivalent automated interchange mechanism), which at least outlines the approved patterns and protocols. DoD Components identify existing APIs and update to the standard.	Functional	Intersects With	Application Programming Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application Programming Interfaces (APIs).	8	
6.6.3	Standardized API Calls & Schemas Pt2	DoD Components will ensure that all ZT applications/services (i.e., PEP, PDP, PIP) adopt the API standard. Information Systems required to follow ZT Target or Advanced Levels prioritize integration with the API standard to simplify automation.	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	
6.6.3	Standardized API Calls & Schemas Pt2	DoD Components will ensure that all ZT applications/services (i.e., PEP, PDP, PIP) adopt the API standard. Information Systems required to follow ZT Target or Advanced Levels prioritize integration with the API standard to simplify automation.	Functional	Intersects With	Application Programming Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application Programming Interfaces (APIs).	8	
6.7	Security Operations Center (SOC) & Incident Response (IR)	In the event a computer network defense service provider (CNDSP) does not exist, DoD organizations define and stand up security operations centers (SOC) to deploy, operate, and maintain security monitoring, protections and response for DAAS; SOCs provide security management visibility for status (upward visibility) and tactical implementation (downward visibility). Workflows within the SOC are automated using automation tooling and enrichment occurs between service providers and technologies.	Functional	Subset Of	Security Operations Center (SOC)	OPS-04	Mechanisms exist to establish and maintain a Security Operations Center (SOC) that facilitates a 24x7 response capability.	10	
6.7.1	Workflow Enrichment Pt1	DoD Enterprise works with Components to establish cybersecurity incident response guidance using industry best practices, such as NIST and a list of approved threat data sources as specified in "Cyber Threat Intelligence Program Pt 1". DoD Components enable workflows for security events using internal context, past threat events, and other threat intelligence. Approved external sources of enrichment are identified for future integration. These workflows are used to determine incident response procedures.	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	
6.7.1	Workflow Enrichment Pt1	DoD Enterprise works with Components to establish cybersecurity incident response guidance using industry best practices, such as NIST and a list of approved threat data sources as specified in "Cyber Threat Intelligence Program Pt 1". DoD Components enable workflows for security events using internal context, past threat events, and other threat intelligence. Approved external sources of enrichment are identified for future integration. These workflows are used to determine incident response procedures.	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	
6.7.2	Workflow Enrichment Pt2	DoD Components identify and establish extended workflows for additional incident response types in alignment with the activity "Threat Alerting Pt 2". Initial enrichment data sources are used for existing workflows. Additional enrichment sources (e.g., UAM, UEBA, profiles, and baselines) are identified for future integrations.	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
6.7.2	Workflow Enrichment Pt2	DoD Components identify and establish extended workflows for additional incident response types in alignment with the activity "Threat Alerting Pt 2". Initial enrichment data sources are used for existing workflows. Additional enrichment sources (e.g., UAM, UEBA, profiles, and baselines) are identified for future integrations.	Functional	Intersects With	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	8	
6.7.3	Workflow Enrichment Pt3	DoD Components use enrichment data sources on basic and extended threat response workflows.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	8	

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
6.7.4	Automated Workflow	DoD Components focus on automating Security Orchestration, Automation, and Response (SOAR) functions and playbooks. Manual processes within security operations are identified and fully automated as possible. Remaining manual processes are decommissioned when possible or marked for exception using a risk-based approach.	Functional	Intersects With	Business Process Task Enumeration	AAT-32.1	Mechanisms exist to identify and enumerate business process task activities that can be executed both manually and in an automated fashion.	8	
6.7.4	Automated Workflow	DoD Components focus on automating Security Orchestration, Automation, and Response (SOAR) functions and playbooks. Manual processes within security operations are identified and fully automated as possible. Remaining manual processes are decommissioned when possible or marked for exception using a risk-based approach.	Functional	Intersects With	Security Orchestration, Automation, and Response (SOAR)	OPS-06	Mechanisms exist to utilize Security Orchestration, Automation and Response (SOAR) tools to define, prioritize and automate the response to security incidents.	8	
7	Visibility and Analytics	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No applicable SCF control
7.1	Log All Traffic (Network, Data, Apps, Users)	DoD organizations collect and process all logs including network, data, application, device, and user logs and make those logs available to the appropriate Computer Network Defense Service Provider (CNDSP) or security operations center (SOC). Logs and events follow a standardized format and rules/analytics are developed as needed.	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	
7.1	Log All Traffic (Network, Data, Apps, Users)	DoD organizations collect and process all logs including network, data, application, device, and user logs and make those logs available to the appropriate Computer Network Defense Service Provider (CNDSP) or security operations center (SOC). Logs and events follow a standardized format and rules/analytics are developed as needed.	Functional	Intersects With	System-Wide / Time-Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.	8	
7.1	Log All Traffic (Network, Data, Apps, Users)	DoD organizations collect and process all logs including network, data, application, device, and user logs and make those logs available to the appropriate Computer Network Defense Service Provider (CNDSP) or security operations center (SOC). Logs and events follow a standardized format and rules/analytics are developed 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.	8	
7.1.1	Scale Considerations	DoD Components conduct analysis to determine current and future scaling needs for monitoring, detection, and response. This requires a prioritization plan aligned with Component business/mission considerations and associated risk alignment. Scaling is analyzed following common industry best practice and aligns with ZT Pillar requirements. The team works with existing Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) groups to determine distributed environment needs in emergencies and Component growth.	Functional	Subset Of	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	10	
7.1.1	Scale Considerations	DoD Components conduct analysis to determine current and future scaling needs for monitoring, detection, and response. This requires a prioritization plan aligned with Component business/mission considerations and associated risk alignment. Scaling is analyzed following common industry best practice and aligns with ZT Pillar requirements. The team works with existing Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) groups to determine distributed environment needs in emergencies and Component growth.	Functional	Intersects With	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	8	
7.1.1	Scale Considerations	DoD Components conduct analysis to determine current and future scaling needs for monitoring, detection, and response. This requires a prioritization plan aligned with Component business/mission considerations and associated risk alignment. Scaling is analyzed following common industry best practice and aligns with ZT Pillar requirements. The team works with existing Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) groups to determine distributed environment needs in emergencies and Component growth.	Functional	Intersects With	Elastic Expansion	CAP-05	Mechanisms exist to automatically scale the resources available for Technology Assets, Applications and/or Services (TAAS), as demand conditions change.	8	
7.1.2	Log Parsing	DoD Components identify and prioritize log and flow sources (e.g., firewalls, Endpoint Detection & Response, Active Directory, switches, routers, etc.) and develop a plan for collection of high-priority logs first, then low-priority. An open industry-standard log format is agreed upon at the DoD Enterprise level with the Components, and implemented in future procurement requirements. Existing solutions and technologies are migrated to this format on a continual basis.	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-01.16	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of Technology Assets, Applications and/or Services (TAAS), based on TAAS criticality and the sensitivity of the data it stores, transmits and processes.	5	
7.1.3	Log Analysis	Enterprise develops common user and device activities. Components identify and prioritize activities based on risk. Events/flows deemed the most simplistic and risky have analytics created using different data sources, such as logs. Trends and patterns are developed over longer periods of time.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	8	
7.1.3	Log Analysis	Enterprise develops common user and device activities. Components identify and prioritize activities based on risk. Events/flows deemed the most simplistic and risky have analytics created using different data sources, such as logs. Trends and patterns are developed over longer periods of time.	Functional	Intersects With	Trend Analysis Reporting	MON-06.2	Mechanisms exist to employ trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.	8	
7.2	Security Information and Event Management (SIEM)	Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) monitor, detect, and analyze data logged into a security information and event management (SIEM) tool. User and device baselines are created using security controls and integrated with the SIEM. Alerting within the SIEM is matured over the phases to support more advanced data points (e.g., Cyber Threat Intel, Baselines, etc.)	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	8	
7.2.1	Threat Alerting Pt1	DoD Components utilize existing Security Information and Event Management (SIEM) solution to develop rules and alerts for common threat events (e.g., malware, phishing, etc.) Alerts and/or rule triggers are fed into the parallel "Asset ID & Alert Correlation" activity to begin automation of responses.	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	5	
7.2.2	Threat Alerting Pt2	DoD Components expand threat alerting in the Security Information and Event Management (SIEM) solution to include Cyber Threat Intelligence (CTI) data feeds. Deviation and anomaly rules are developed in the SIEM to detect advanced threats.	Functional	Subset Of	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	10	
7.2.3	Threat Alerting Pt3	Threat alerting is expanded to include advanced data sources, such as Extended Detection & Response (XDR), User & Entity Behavior Analytics (UEBA), and User Activity Monitoring (UAM). These advanced data sources are used to develop improved anomalous and pattern activity detections.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	8	
7.2.3	Threat Alerting Pt3	Threat alerting is expanded to include advanced data sources, such as Extended Detection & Response (XDR), User & Entity Behavior Analytics (UEBA), and User Activity Monitoring (UAM). These advanced data sources are used to develop improved anomalous and pattern activity detections.	Functional	Intersects With	Integration of Scanning & Other Monitoring Information	MON-02.3	Automated mechanisms exist to integrate the analysis of audit records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further enhance the ability to identify inappropriate or unusual activity.	8	
7.2.4	Asset ID & Alert Correlation	All assets in SIEM are identified and correlated to alerts in order to provide security teams with accurate and detailed information. This information contributes to the incident response speed. Asset ID's also allow better visibility while preforming vulnerability assessments.	Functional	Intersects With	Integration of Scanning & Other Monitoring Information	MON-02.3	Automated mechanisms exist to integrate the analysis of audit records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further enhance the ability to identify inappropriate or unusual activity.	8	
7.2.4	Asset ID & Alert Correlation	All assets in SIEM are identified and correlated to alerts in order to provide security teams with accurate and detailed information. This information contributes to the incident response speed. Asset ID's also allow better visibility while preforming vulnerability assessments.	Functional	Intersects With	Automated Network Asset Discovery	AST-32	Mechanisms exist to automate network asset discovery through Software Defined Networking (SDN), or similar technologies, that analyzes network traffic to:(1) Identify;(2) Document; and(3) Track devices.	5	
7.2.5	User/Device Baselines	DoD Components develop a subject/attribute baseline approach based on typical pattern and behavior in activity "Establish User Baseline Behavior". This approach will serve as a benchmark for security when identifying and responding to abnormal or malicious activity.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	8	
7.2.5	User/Device Baselines	DoD Components develop a subject/attribute baseline approach based on typical pattern and behavior in activity "Establish User Baseline Behavior". This approach will serve as a benchmark for security when identifying and responding to abnormal or malicious activity.	Functional	Intersects With	Behavioral Baselining	THR-11	Automated mechanisms exist to establish behavioral baselines that capture information about user and entity behavior to enable dynamic threat discovery.	8	
7.3	Common Security and Risk Analytics	Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) employ data tools across their enterprises for multiple data types to unify data collection and examine events, activities, and behaviors.	Functional	Subset Of	Security Operations Center (SOC)	OPS-04	Mechanisms exist to establish and maintain a Security Operations Center (SOC) that facilitates a 24x7 response capability.	10	
7.3.1	Implement Analytics Tools	The DOD Enterprise provides minimum requirements for analytics tool capabilities to analyze data across all ZT pillars. Components procure and implement an analytics tool in order to provide actionable insights and intelligence.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
7.3.2	Establish User Baseline Behavior	Utilizing the analytics tools implemented, subject behavior patterns are analyzed to identify patterns and deviations from normality. Techniques in analytics involve machine learning and UEBA.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	8	
7.3.2	Establish User Baseline Behavior	Utilizing the analytics tools implemented, subject behavior patterns are analyzed to identify patterns and deviations from normality. Techniques in analytics involve machine learning and UEBA.	Functional	Intersects With	Behavioral Baselining	THR-11	Automated mechanisms exist to establish behavioral baselines that capture information about user and entity behavior to enable dynamic threat discovery.	8	
7.4	User and Entity Behavior Analytics	DoD organizations initially employ analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors and detect anomalies. Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) mature this capability through the employment of advanced analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors, and detect anomalies.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	8	
7.4	User and Entity Behavior Analytics	DoD organizations initially employ analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors and detect anomalies. Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) mature this capability through the employment of advanced analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors, and detect anomalies.	Functional	Intersects With	Behavioral Baselining	THR-11	Automated mechanisms exist to establish behavioral baselines that capture information about user and entity behavior to enable dynamic threat discovery.	8	
7.4.1	Baseline & Profiling Pt1	Utilizing the baselines developed in the "User/Device Baselines" activity, threat profiles are created to assess the level of risk for individual subjects associated to the overall Component security. Profiles should be integrated into the "Orgnization Access Profile" activity for decision making.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	8	

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
7.4.2	Baseline & Profiling Pt2	DoD Components expand baselines and profiles to include unmanaged and non-standard device types, including Internet of Things (IoT) and Operational Technology (OT), through data output monitoring. These devices are again profiled based on standardized attributes and use cases. Analytics are updated to consider the new baselines and profiles, accordingly enabling further detections and response. Specific risky users and devices are automatically prioritized for increased monitoring based on risk. Detection and response are integrated with cross pillar functionalities.	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	
7.4.2	Baseline & Profiling Pt2	DoD Components expand baselines and profiles to include unmanaged and non-standard device types, including Internet of Things (IoT) and Operational Technology (OT), through data output monitoring. These devices are again profiled based on standardized attributes and use cases. Analytics are updated to consider the new baselines and profiles, accordingly enabling further detections and response. Specific risky users and devices are automatically prioritized for increased monitoring based on risk. Detection and response are integrated with cross pillar functionalities.	Functional	Intersects With	Behavioral Baselining	THR-11	Automated mechanisms exist to establish behavioral baselines that capture information about user and entity behavior to enable dynamic threat discovery.	5	
7.4.3	UEBA Baseline Support Pt 1	User & Entity Behavior Analytics (UEBA) within DoD Components expands monitoring to advanced analytics such as Machine Learning (ML). These results are in turn reviewed and provided back into ML algorithms to improve detection and response.	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	
7.4.4	UEBA Baseline Support Pt 2	User & Entity Behavior Analytics (UEBA) within DoD Components completes it expansion by using traditional and Machine Learning (ML) based results to be provided to Artificial Intelligence (AI) algorithms. AI based detections are supervised, but ultimately, using advanced techniques such as neural networks, UEBA operators are not part of the learning process.	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	
7.5	Threat Intelligence Integration	Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) integrate threat intelligence information and streams about identities, motivations, characteristics, and tactics, techniques and procedures (TTPs) with data collected in the SIEM.	Functional	Subset Of	Security Operations Center (SOC)	OPS-04	Mechanisms exist to establish and maintain a Security Operations Center (SOC) that facilitates a 24x7 response capability.	10	
7.5	Threat Intelligence Integration	Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) integrate threat intelligence information and streams about identities, motivations, characteristics, and tactics, techniques and procedures (TTPs) with data collected in the SIEM.	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.	8	
7.5.1	Cyber Threat Intelligence Program Pt1	The DoD Enterprise works with Components to develop a Cyber Threat Intelligence (CTI) program policy, standard, and process. Components utilize this documentation to develop organizational CTI teams with key mission/task stakeholders. CTI teams gather intelligence from common data feeds across ZT Pillars and aggregate all intelligence to a centralized repository (e.g. SIEM).	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.	8	
7.5.2	Cyber Threat Intelligence Program Pt2	DoD Components expand their Cyber Threat Intelligence (CTI) teams to include new stakeholders as appropriate. Existing and authenticated, private and controlled threat intelligence is analyzed, and appropriate actions and controls are enforced across ZT Pillars. CTI Program adapts strategy over time with expansion of threat intelligence developed in solutions and program maturity.	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.	8	
7.6	Automated Dynamic Policies	DoD Organization ML & AI solutions dynamically and automatically update security profiles and device configuration through continuous security posture monitoring, risk and confidence scoring, and automated patch management.	Functional	Intersects With	Robotic Process Automation (RPA)	AAT-32	Mechanisms exist to implement Robotic Process Automation (RPA) to improve efficiency, accuracy and speed for high-volume, repetitive and rules-based business processes.	8	