DoD Zero Trust Capability Execution Roadmap (COA 1)

06 January 2023

Notes:

1. Although applicable to all the DoD, including Components that own and operate National Security Systems (NSS), this Strategy does not impact the authority and responsibilities of the Director of the National Security Agency (NSA) in connection with the National Manager responsibilities for NSS assigned to the Director of the NSA by National Security Directive 42 (NSD-42), *National Policy for the Security of National Security Telecommunications and Information Systems* , 5 July 1990. The NSS National Manager rather than the DoD sets NSS Zero Trust guidance.

2. The DoD Zero Trust Capability Roadmap described in the High-Level Capability Roadmap section below provides a guide to follow for the DoD baseline course of action (COA). Additionally, to accelerate Zero Trust adoption, the Department is considering several additional complementary COAs including commercial and Government-owned cloud-based enterprise services

DoD Zero Trust Capabilities

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Associated Activities
1.1	User Inventory	1 - User	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.	System owners have control (visibility and administrative rights) of all authorized and authenticated users on the network	Users not on the authorized user list will be denied access by policy	* Inventory User
1.2	Conditional User Access	1 - User	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.	Eventually, organizations control user, device, and non-user entity DAAS access through dynamically changing user risk profiles and fine grained access control to include the use of user risk assessments	Users not known to the system and users who present an unacceptable degree of risk will be denied access with greater accuracy	* Implement App Based Permissions per Enterprise * Rule Based Dynamic Access Pt1 * Rule Based Dynamic Access Pt2 * Enterprise Gov't roles and Permissions Pt1 * Enterprise Gov't roles and Permissions Pt2
1.3	Multi-Factor Authentication (MFA)	1 - User	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.	DoD organizations require users and non-user entities to authenticate using at least two of the following three attributes: knowledge (user ID/password), possession (CAC/token), or something you are (inherence, e.g., iris/fingerprints), in order to access DAAS	Users not presenting multiple forms of authentication will be denied access to DAAS system and resources	* Organizational MFA/IDP * Alternative Flexible MFA Pt1 * Alternative Flexible MFA Pt2
1.4	Privileged Access Management (PAM)	1 - User	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.	DoD organizations control, monitor, secure, and audit privileged identities (e.g., through password vaulting, JIT/JEA with PAWS) across their IT environments	Critical assets and applications secured, controlled, monitored and managed through limits on admin access	* Implement System and Migrate Privileged Users Pt1 * Implement System and Migrate Privileged Users Pt2 * Real time Approvals & JIT/JEA Analytics Pt1 * Real time Approvals & JIT/JEA Analytics Pt2
1.5	Identity Federation & User Credentialing	1 - User	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.	DoD organizations manually issue, manage, and revoke credentials bound to DoD person, device, and NPE identities. Identity information is developed and shared across entitles and trust domains providing "single sign-on" convenience and efficiencies to identified (authenticated and authorized) users and devices.	Visibility and accuracy of user authentication information is increased, to include DoD users and users managed by other agencies. Users lacking sufficient credentials are denied access according to established policies.	* Organizational Identity Life-Cycle Management * Enterprise Identity Life-Cycle Management Pt1 * Enterprise Identity Life-Cycle Management Pt2 * Enterprise Identity Life-Cycle Management Pt3
1.6	Behavioral, Contextual ID, and Biometrics	1 - User	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.	DoD organizations utilize behavioral, contextual, and biometric telemetry to enhance risk-based authentication and access controls	Behavioral, contextual, and biometric telemetry enhances MFA with	* Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling * User Activity Monitoring Pt1 * User Activity Monitoring Pt2
1.7	Least Privileged Access	1 - User	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.	DoD organizations govern access to DAAS using the absolute minimum access required to perform routine, legitimate tasks or activities	Users on the network only have access to the DAAS for which they are authorized and authenticated over a specific timeframe	* Deny User by Default Policy
1.8	Continuous Authentication	1 - User	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.	DoD organizations continuously authenticate and authorize users' access to DAAS within and across sessions using MFA	Users not continuously presenting multiple forms of authentication will be denied access to DAAS system and resources	* Single Authentication * Periodic Authentication * Continuous Authentication Pt1 * Continuous Authentication Pt2

DoD Zero Trust Capabilities

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Associated Activities
1.9	Integrated ICAM Platform	1 - User	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.	DoD organizations employ enterprise-level identity management systems to track user 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	Identities of users and NPE are centrally managed to ensure authorized and authenticated access to DAAS resources across platforms	* Enterprise PKI/IDP Pt1 * Enterprise PKI/IDP Pt2 * Enterprise PKI/IDP Pt3
2.1	Device Inventory	2 - Device	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.	DoD organizations establish and maintain a trusted inventory list of all devices authorized to access the network and enroll all devices on the network prior to network connection	By default policy, devices will be denied network access; the only devices permitted access to the network shall be known, authorized, and listed in the device inventory	* Device Health Tool Gap Analysis * NPE/PKI, Device under Management * Enterprise IDP Pt1 * Enterprise IDP Pt2
2.2	Device Detection and Compliance	2 - Device	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)	DoD organizations employ asset management systems for user devices to maintain and report on IT compliance. Any device (including mobile, IOT, managed, and unmanaged) attempting to connect to a DoD network or access a DAAS resource is detected and has its compliance status confirmed (via C2C)	Any device attempting to connect to the network will be detected; only those devices that are compliant (e.g., anti-virus is up to date, approved configuration) will receive access to requested DAAS	* Implement C2C/Compliance Based Network Authorization Pt1 * Implement C2C/Compliance Based Network Authorization Pt2
2.3	Device Authorization w/ Real Time Inspection	2 - Device	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.	DoD organizations establish processes (e.g., Enterprise PKI) and utilize tools to identify any device (including unmanaged devices, infrastructure devices, and endpoint devices) attempting to access the network, and make a determination if the device should be authorized to access the network. Maturation of this capability monitoring and detection of this activity on endpoints and IT infrastructure in real time	Components can use policies to deny devices by default and explicitly allow access to DAAS resources only by devices that meet mandated configuration standards. Security threats identified are remediated faster through continuous activity inspection enables faster remediation of security threats	* Entity Activity Monitoring Pt1 * Entity Activity Monitoring Pt2 * Implement Application Control & File Integrity Monitoring (FIM) Tools * Integrate NextGen AV Tools with C2C * Fully Integrate Device Security stack with C2C as appropriate * Enterprise PKI Pt1 * Enterprise PKI Pt2
2.4	Remote Access	2 - Device	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.	DoD organizations establish policies to allow authorized users and devices access to the network or a device from a geographical distance through a network connection	Enables properly authorized and authenticated users and NPEs to access DAAS from remote locations	* Deny Device by Default Policy * Managed and Limited BYOD & IOT Support * Managed and Full BYOD & IOT Support Pt1 * Managed and Full BYOD & IOT Support Pt2
2.5	Partially & Fully Automated Asset, Vulnerability and Patch Management	2 - Device	DoD organizations establish processes to automatically test and deploy vendor patches for connected devices; hybrid patch management (both human and automated) is employed	DoD organizations establish processes to automatically test and deploy vendor patches for connected devices; hybrid patch management (both human and automated) is employed	Risk is minimized by automatically deploying vendor patches to all network devices	* Implement Asset, Vulnerability and Patch Management Tools
2.6	Unified Endpoint Management (UEM) & Mobile Device Management (MDM)	2 - Device	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.	DoD organizations establish a centralized UEM tool that provides the choices of agent and/or agentless management of computer and mobile devices to a single console. DoD-issued mobile devices are remotely managed and security policies are enforced.	DAAS resources are protected through agent and agentless management, IT is able to manage, secure, and deploy resources and applications on any device from a single console to provide redress of cybersecurity threats. Security vulnerabilities are mitigated and policy enforcement measures are received through IT remote management of DoD-issued mobile devices	* Implement UEDM or equivalent Tools * Enterprise Device Management Pt1 * Enterprise Device Management Pt2

DoD Zero Trust Capabilities

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Associated Activities
2.7	Endpoint & Extended Detection & Response (EDR & XDR)	2 - Device	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.	DoD organizations use EDR tools to monitor, detect, and remediate malicious activity on endpoints as a baseline. Upgrading to XDR tools allows organizations to account for activity beyond the endpoints.	Threats originating from network-connected endpoints are initially reduced through active investigation and response. Maturation focuses on forensics and faster threat detection and remediation are enabled by correlating data across multiple security layers (e.g., email, cloud, endpoint)	* Implement Endpoint Detection & Response (EDR) Tools and Integrate with C2C * Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt1 * Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt2
3.1	Application Inventory	3 - Applications and Workloads	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	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	Unauthorized applications and application components are not used on or within the system	* Application/Code Identification
3.2	Secure Software Development & Integration	3 - Applications and Workloads	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.	Organization-defined security controls and practices are integrated, to include Zero Trust security controls and virtualization, into the software development lifecycle and DevOps toolchain. Custom software development teams use DevSecOps to integrate static and dynamic application security testing into software delivery workflows in accordance with the organization's requirements (policies, technologies, and processes).	Zero Trust security concepts, processes, and capabilities are accepted and integrated across the DevOps toolchain, to include static and dynamic application security testing necessary for the discovery of weaknesses and vulnerabilities during application development	* Build DevSecOps Software Factory Pt1 * Build DevSecOps Software Factory Pt2 * Automate Application Security & Code Remediation Pt1 * Automate Application Security & Code Remediation Pt2
3.3	Software Risk Management	3 - Applications and Workloads	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.	DoD establishes policies and procedures to secure supply chain cybersecurity for code components within DoD and DIB systems by evaluating and identifying supplier sourcing risk for approved sources, creating repositories and update channels for use by development teams, creating Bill of Materials for applications to identify source, supportability and risk posture, and establishing industry standard (DIB) and approved vulnerability databases for use in DevSecOps	Code used in DAAS and associated components of the supply chain is secure, vulnerabilities are reduced, and DoD is aware of potential risks	* Approved Binaries/Code * Vulnerability Management Program Pt1 * Vulnerability Management Program Pt2 * Continual Validation
3.4	Resource Authorization & Integration	3 - Applications and Workloads	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.	DoD establishes a standard approach managing the authorizations of resources in a risk approach that reviews the User, Device and Data security posture.	Resource authorization enables the ability for limited access to those resources and in a programmatic way in later stages. This improvise the ability to remove access when it is not needed.	* Resource Authorization Pt1 * Resource Authorization Pt2 * SDC Resource Authorization Pt1 * SDC Resource Authorization Pt2 * Enrich Attributes for Resource Authorization Pt1 * Enrich Attributes for Resource Authorization Pt2 * REST API Micro-Segments
3.5	Continuous Monitoring and Ongoing Authorizations	3 - Applications and Workloads	DoD organizations employ automated tools and processes to continuously monitor applications and assess their authorization to operate	DoD organizations employ automated tools and processes to continuously monitor applications and assess their authorization to operate	Near real time visibility into the effectiveness of deployed security controls	* Continuous Authorization to Operate (cATO) Pt1 * Continuous Authorization to Operate (cATO) Pt2
4.1	Data Catalog Risk Alignment	4 - Data	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	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	Data assets are known and can therefore be collected, tagged, and protected according to risk levels in alignment with a prioritization framework, and encrypted for protection	* Data Analysis

DoD Zero Trust Capabilities

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Associated Activities
4.2	DoD Enterprise Data Governance	4 - Data	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.	DoD establishes enterprise data labeling/tagging and DAAS access control/sharing policies (e.g., SDS policy) that are enforceable at the field level	Decision rights and accountability framework ensure appropriate behavior in the valuation, creation, consumption, and control of data and analytics	* Define Data Tagging Standards * Interoperability Standards * Develop Software Defined Storage (SDS) Policy
4.3	Data Labeling and Tagging	4 - Data	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.	Data owners label and tag data in compliance with DoD enterprise governance on labeling/tagging policy	Establishing machine enforceable data access controls, risk assessment, and situational awareness require consistently and correctly labeled and tagged data	* Implement Data Tagging & Classification Tools * Manual Data Tagging Pt1 * Manual Data Tagging Pt2 * Automated Data Tagging & Support Pt1 * Automated Data Tagging & Support Pt2
4.4	Data Monitoring and Sensing	4 - Data	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.	Data owners will capture active metadata that includes information about the access, sharing, transformation, and use of their data assets	Data in all states are detectable and observable	* DLP Enforcement Point Logging and Analysis * DRM Enforcement Point Logging and Analysis * File Activity Monitoring Pt1 * File Activity Monitoring Pt2 * Database Activity Monitoring * Comprehensive Data Activity Monitoring
4.5	Data Encryption & Rights Management	4 - Data	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	DoD organizations establish and implement a strategy for encrypting data at rest and in transit	Encrypting data in all states reduces the risk of unauthorized data access and improves data security	* Implement DRM and Protection Tools Pt1 * Implement DRM and Protection Tools Pt2 * DRM Enforcement via Data Tags and Analytics Pt1 * DRM Enforcement via Data Tags and Analytics Pt2 * DRM Enforcement via Data Tags and Analytics Pt3
4.6	Data Loss Prevention (DLP)	4 - Data	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.	DoD organizations have identified enforcement points, deployed approved DLP tools at those enforcement points, and integrate tagged data attributes with DLP	Data breaches and data exfiltration transmissions are detected and mitigated	* Implement Enforcement Points * DLP Enforcement via Data Tags and Analytics Pt1 * DLP Enforcement via Data Tags and Analytics Pt2 * DLP Enforcement via Data Tags and Analytics Pt3
4.7	Data Access Control	4 - Data	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.	DoD organizations ensure appropriate access to and use of data based on the data and user/NPE/device properties	Unauthorized entities, or any entity on an unauthorized device cannot access data; Zero Trust cybersecurity will be sufficiently strong to separate community of interest data access for data in the same classification	* Integrate DAAS Access w/ SDS Policy Pt1 * Integrate DAAS Access w/ SDS Policy Pt2 * Integrate DAAS Access w/ SDS Policy Pt3 * Integrate Solution(s) and Policy with Enterprise IDP Pt1 * Integrate Solution(s) and Policy with Enterprise IDP Pt2 * Implement SDS Tool and/or integrate with DRM Tool Pt1 * Implement SDS Tool and/or integrate with DRM Tool Pt2
5.1	Data Flow Mapping	5 - Network and Environment	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.	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	Sets the foundation for network segmentation and tighter access control by understanding data traffic on the network	* Define Granular Control Access Rules & Policies Pt1 * Define Granular Control Access Rules & Policies Pt2
5.2	Software Defined Networking (SDN)	5 - Network and Environment	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.	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	Enables the control of packets to a centralized server, provides additional visibility into the network, and enables integration requirements	* Define SDN APIs* Implement SDN Programable Infrastructure * Segment Flows into Control, Management, and Data Planes * Network Asset Discovery & Optimization * Real-Time Access Decisions
5.3	Macro Segmentation	5 - Network and Environment	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.	DoD organizations establish network perimeters and provide security against devices located within an environment by validating the device, user, or NPE on each attempt of accessing a remote resource prior to connection	Network segmentation is defined by a large perimeter to enable resource segmentation by function and user type	* Datacenter Macro segmentation * B/C/P/S Macro segmentation

DoD Zero Trust Capabilities

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Associated Activities
5.4	Micro Segmentation	5 - Network and Environment	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.	DoD organizations define and document network segmentation based on identity and / or application access in their virtualized cloud environments	Network segmentation enabled by narrower and specific segmentation in a virtualized environment via identity and / or application access, allowing for improved protection of data in transit as it crosses system boundaries (e.g., in a coalition environment, system high boundaries) and supported dynamic, real-time access decisions and policy changes	* Implement Micro segmentation * Application & Device Micro segmentation * Process Micro segmentation * Protect Data In Transit
6.1	Policy Decision Point (PDP) & Policy Orchestration	6 - Automation and 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.	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	PDPs and PEPs ensure proper implementation of DAAS access policies to users or endpoints that are properly connected (or denied access) to requested resources	* Policy Inventory & Development * Organization Access Profile * Enterprise Security Profile Pt1 * Enterprise Security Profile Pt2
6.2	Critical Process Automation	6 - Automation and Orchestration	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.	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	Response time and capability is increased with orchestrated workflows and risk management processes	* Task Automation Analysis * Enterprise Integration & Workflow Provisioning Pt1 * Enterprise Integration & Workflow Provisioning Pt2
6.3	Machine Learning	6 - Automation and Orchestration	DoD organizations employ ML to execute (and enhance execution of) critical functions such as incident response, anomaly detection, user baselining, and data tagging.	DoD organizations employ ML to execute (and enhance execution of) critical functions such as incident response, anomaly detection, user baselining, and data tagging	Response time and capability is increased with orchestrated workflows and risk management processes	* Implement Data Tagging & Classification ML Tools
6.4	Artificial Intelligence	6 - Automation and Orchestration	DoD organizations employ AI to execute (and enhance execution of) critical functions - particularly risk and access determinations and environmental analysis.	DoD organizations employ AI to execute (and enhance execution of) critical functions - particularly risk and access determinations and environmental analysis	Response time and capability is increased with orchestrated workflows and risk management processes	* Implement AI automation tools * AI Driven by Analytics decides A&O modifications
6.5	Security Orchestration, Automation & Response (SOAR)	6 - Automation and Orchestration	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.	DoD organizations achieve IOC 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	Pre-defined playbooks from collection to incident response and triage enables initial process automation that accelerates a security team's decision and response speed	* Response Automation Analysis * Implement SOAR Tools * Implement Playbooks
6.6	API Standardization	6 - Automation and Orchestration	DoD establishes and enforces enterprise-wide programmatic interface (e.g., API) standards; all non-compliant APIs are identified and replaced.	DoD establishes and enforces enterprise-wide API standards; all non-compliant APIs are identified and replaced	Standardizing APIs across the department improves application interfaces, enabling orchestration, and enhancing interoperability	* Tool Compliance Analysis * Standardized API Calls & Schemas Pt1 * Standardized API Calls & Schemas Pt2
6.7	Security Operations Center (SOC) & Incident Response (IR)	6 - Automation and Orchestration	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.	In the event a CNDSP does not exist, DoD organizations define and stand up SOCs 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)	Standardized, coordinated, and accelerated incident response and investigative efforts	* Workflow Enrichment Pt1 * Workflow Enrichment Pt2 * Workflow Enrichment Pt3 * Automated Workflow

DoD Zero Trust Capabilities

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Associated Activities
7.1	Log All Traffic (Network, Data, Apps, Users)	7 - Visibility and Analytics	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.	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 SOC	Foundational to the development of automated hunt and incident response playbooks	* Scale Considerations * Log Parsing * Log Analysis
7.2	Security Information and Event Management (SIEM)	7 - Visibility and Analytics	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.)	CNDSPs/SOCs monitor, detect, and analyze data logged into a security information and event management (SIEM) tool	Processing and exploiting data in the SIEM enables effective security analysis of anomalous user behavior, alerting, and automation of relevant incident response to common threat events	* Threat Alerting Pt1 * Threat Alerting Pt2 * Threat Alerting Pt3 * Asset ID & Alert Correlation * User/Device Baselines
7.3	Common Security and Risk Analytics	7 - Visibility and 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.	CNDSPs/SOCs employ big data tools across their enterprises for multiple data types to unify data collection and examine events, activities, and behaviors	Analysis integrated across multiple data types to examine event, activities, and behaviors	* Implement Analytics Tools * Establish User Baseline Behavior
7.4	User and Entity Behavior Analytics	7 - Visibility and 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.	DoD organizations initially employ analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors, and detect anomalies. CNDSPs/SOCs 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	Advanced analytics support detection of anomalous users, devices, and NPE actions and advanced threats	* Baseline & Profiling Pt1 * Baseline & Profiling Pt2 * UEBA Baseline Support Pt1 * UEBA Baseline Support Pt2
7.5	Threat Intelligence Integration	7 - Visibility and Analytics	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.	CNDSPs/SOCs integrate threat intelligence information and streams about identities, motivations, characteristics, and tactics, techniques and procedures (TTPs) with data collected in the SIEM	Integrating threat intelligence into other SIEM data enhances monitoring efforts and incident response	* Cyber Threat Intelligence Program Pt1 * Cyber Threat Intelligence Program Pt2
7.6	Automated Dynamic Policies	7 - Visibility and Analytics	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.	CNDSPs/SOCs dynamically and automatically update security profiles and device configuration through continuous security posture monitoring, risk and confidence scoring, and automated patch management	Users and NPEs are denied access based on automated, real-time security profiles based on external conditions and evolving risk and confidence scores	* AI-enabled Network Access * AI-enabled Dynamic Access Control

DoD Zero Trust Activities

ID#	Activity Name	Associated Capability	Phase	Duration (months)	Descriptions	Outcomes	Predecessor(s)	Successor(s)
1.1.1	Inventory User	1.1 User Inventory	Target Level ZT	25.9	DoD Organizations establish and update a user inventory manually if needed, preparing for automated approach in later stages. Accounts both centrally managed by an IdP/ICAM and locally on systems will be identified and inventoried. Privileged accounts will be identified for future audit and both standard and privileged user accounts local to applications and systems will be identified for future migration and/or decommission.	Identified Managed Regular Users; Identified Managed Privileged Users; Identified applications using their own user account management for non-administrative and administrative accounts		
1.2.1	Implement App Based Permissions per Enterprise	1.2 Conditional User Access	Target Level ZT	17.7	The DoD enterprise working with the Organizations establishes a basic 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 is enabled for self-service functionality for adding/updating attributes within the solution. Remining Privileged Access Management (PAM) activities are fully migrated to PAM solution.	Enterprise roles/attributes needed for user authorization to application functions and/or data have been registered with enterprise ICAM; DoD Enterprise ICAM has self-service attribute/role registration service that enables application owners to add attributes or use existing enterprise attributes; Privileged activities are fully migrated to PAM		
1.2.2	Rule Based Dynamic Access Pt1	1.2 Conditional User Access	Target Level ZT	22.1	DoD Organizations utilize the rules from the "Periodic Authentication" activity to build basic rules enabling and disabling privileges dynamically. High-risk user accounts utilize the PAM solution to move to dynamic privileged access using Just-In-Time access and Just-Enough-Administration methods.	Access to application's/service's functions and/or data are limited to users with appropriate enterprise attributes; All possible applications use JIT/JEA permissions for administrative users	Single Authentication	Rule Based Dynamic Access Pt2; AI-enabled Network Access
1.2.3	Rule Based Dynamic Access Pt2	1.2 Conditional User Access	Advanced ZT	15.5	DoD Organizations 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 and Artificial Intelligence functionality enabling automated rule management.	Components and services are fully utilizing rules to enable dynamic access to applications and services; Technology utilized for Rule Based Dynamic Access supports integration with AI/ML tooling	Rule Based Dynamic Access Pt1; File Activity Monitoring Pt2	
1.2.4	Enterprise Gov't roles and Permissions Pt1	1.2 Conditional User Access	Advanced ZT	11.6	DoD Organizations 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 Identity, Credential and Access Management (ICAM) solutions are migrated to cloud services and/or environments enabling improved resilience and performance.	Component attribute and role data repository federated with enterprise ICAM; Cloud-based enterprise IdP can be used by cloud and on-premises applications; A standardized set of roles and permissions are created and aligned to attributes		Enterprise Gov't roles and Permissions Pt2
1.2.5	Enterprise Gov't roles and Permissions Pt2	1.2 Conditional User Access	Advanced ZT	11.2	DoD Organizations move all possible functions of the Identity Provider (IdP) and Identity, Credential and Access Management (ICAM) solutions to cloud environments. Enclave/DDIL environments local capabilities to support disconnected functions but ultimately are managed by the centralized Identity, Credential and Access Management (ICAM) solutions. Updated roles are now mandated for usage and exceptions are reviewed following a risk-based approach.	Majority of components utilize cloud IdP functionality Where possible on-prem IdP is decommissioned; Permissions and roles are mandated for usage when evaluating attributes	Enterprise Gov't roles and Permissions Pt1	
1.3.1	Organizational MFA/IDP	1.3 Multi-Factor Authentication (MFA)	Target Level ZT	10.6	DoD Organizations procure and implement a centralized Identity Provider (IdP) solution and Multi-Factor (MFA) solution. 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 enabling key pairs to be signed by the trusted root certificate authorities. Mission/Task-Critical applications and services are utilizing the IdP and MFA solution for management of users and groups.	Component is using IdP with MFA for critical applications/services; Components have implemented an Identity Provider (IdP) that enables DoD PKI multifactor authentication; Organizational Standardized PKI for critical services		Alternative Flexible MFA Pt1
1.3.2	Alternative Flexible MFA Pt1	1.3 Multi-Factor Authentication (MFA)	Advanced ZT	17.4	DoD Organization's Identity Provider (IdP) supports alternative methods of multi-factor authentication complying with Cyber Security requirements (e.g., FIPS 140-2, FIPS 197, etc.). Alternative tokens can be used for application-based authentication. Multi-Factor options support Biometric capability and can be managed using a self-service approach. Where possible multi-factor provider(s) is moved to cloud services instead of being hosted on-premise.	IdP provides user self-service alternative token; IdP provides alt token MFA for approved applications per policy	Organizational MFA/IDP	Alternative Flexible MFA Pt2

ID#	Activity Name	Associated Capability	Phase	Duration (months)	Descriptions	Outcomes	Predecessor(s)	Successor(s)
1.3.3	Alternative Flexible MFA Pt2	1.3 Multi-Factor Authentication (MFA)	Advanced ZT	14.6	Alternative tokens 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). This functionality is further extended onto Biometric enabled alternative tokens as well.	User Activity Patterns Implemented	Alternative Flexible MFA Pt1	
1.4.1	Implement System and Migrate Privileged Users Pt1	1.4 Privileged Access Management (PAM)	Target Level ZT	12.4	DoD Organizations procure and implement a Privileged Access Management (PAM) solution 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 PAM solution are transitioned over to using solution versus static and direct privileged permissions.	Privilege Access Management (PAM) tooling is implemented; applications and devices that support and do not support PAM tools identified; Applications that support PAM, now use PAM for controlling emergency/built-in accounts		Implement System and Mitigate Privileged Users Pt2
1.4.2	Implement System and Migrate Privileged Users Pt2	1.4 Privileged Access Management (PAM)	Target Level ZT	14.4	DoD Organizations utilize the inventory of supported and unsupported Applications/Services for integration with 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 PAM solution.	Privileged activities are migrated to PAM and access is fully managed	Implement System and Mitigate Privileged Users Pt1	Real time Approvals & JIT/JEA Analytics Pt1
1.4.3	Real time Approvals & JIT/JEA Analytics Pt1	1.4 Privileged Access Management (PAM)	Advanced ZT	12.5	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.	Identified accounts, applications, devices, and data of concern (of greatest risk to DoD mission); Using PAM tools, applied JIT/JEA access to high-risk accounts; Privileged access requests are automated as appropriate	Implement System and Mitigate Privileged Users Pt2	Real time Approvals & JIT/JEA Analytics Pt2
1.4.4	Real time Approvals & JIT/JEA Analytics Pt2	1.4 Privileged Access Management (PAM)	Advanced ZT	8.9	DoD Organizations 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.	UEBA or similar analytic system integrated with PAM tools for JIT/JEA account approvals	Real time Approvals & JIT/JEA Analytics Pt1	
1.5.1	Organizational Identity Life-Cycle Management	1.5 Identity Federation & User Credentialing	Target Level ZT	14.8	DoD Organizations establish a process for life cycle management of users both privileged and standard. Utilizing the Organizational Identity Provider (IdP) the process is implemented and followed by the maximum number of users. Any users who fall outside of the standard process are approved through risk-based exceptions to be evaluated regularly for decommission.	Standardized Identity Lifecycle Process		Enterprise Identity Life-cycle Management Pt1
1.5.2	Enterprise Identity Life-Cycle Management Pt1	1.5 Identity Federation & User Credentialing	Target Level ZT	11.7	The DoD Enterprise works with Organizations to review and align the existing Identity Lifecycle Processes, policy, and standards. A finalized agreed upon policy and supporting process are developed and followed by the DoD Organizations. Utilizing the centralized or federated Identity Provider (IdP) and Identity & Access Management (IdAM) solutions, DoD Organizations implement the Enterprise Lifecycle Management process for the maximum number of identities, groups, and permissions. Exceptions to the policy are managed in a risk based methodical approach.	Automated Identity Lifecycle Processes; Integrated with Enterprise ICAM process and tools	Organization Identity Life-cycle Management	Enterprise Identity Life-cycle Management Pt2
1.5.3	Enterprise Identity Life-Cycle Management Pt2	1.5 Identity Federation & User Credentialing	Advanced ZT	12.8	DoD Organizations further integrate the critical automation functions of the Identity Provider (IdP) and Identity, Credential and Access Management (ICAM) solutions following the Enterprise Lifecycle Management process to enable Enterprise automation and analytics. Identity Lifecycle Management primary processes are integrated into the cloud-based Enterprise ICAM solution.	Integration w/ Critical IDM/IDP functions; Primary ILM functions are cloud based	Enterprise Identity Life-cycle Management Pt1	Enterprise Identity Life-cycle Management Pt3
1.5.4	Enterprise Identity Life-Cycle Management Pt3	1.5 Identity Federation & User Credentialing	Advanced ZT	9.2	DoD Organizations integrate remaining Identity Lifecycle Management processes with the Enterprise Identity, Credential and Access Management solution. Enclave/DDIL environments while still authorized to operate integrate with the Enterprise ICAM using local connectors to the cloud environment.	All ILM functions moved to cloud as appropriate; Integration with all IDM/IDP functions	Enterprise Identity Life-cycle Management Pt2	
1.6.1	Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling	1.6 Behavioral, Contextual ID, and Biometrics	Target Level ZT	15.9	DoD Organizations 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.	UEBA and UAM functionality is implemented for Enterprise IDP		Establish User Baseline Behavior; Baseline & Profiling Pt1

DoD Zero Trust Activities

ID#	Activity Name	Associated Capability	Phase	Duration (months)	Descriptions	Outcomes	Predecessor(s)	Successor(s)
1.6.2	User Activity Monitoring Pt1	1.6 Behavioral, Contextual ID, and Biometrics	Advanced ZT	13.5	DoD Organizations integrate User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions with Organizational Identity Providers (IdP) for extended visibility as needed. Analytics and data generated by UEBA and UAM for critical applications/services are integrated with the Just-in-Time and Just-Enough-Access solution improving decision making further.	UEBA is integrated with Org IDPs as appropriate; UEBA is integrated with JIT/JEA for critical services	User/Device Baselines	User Activity Monitoring Pt2
1.6.3	User Activity Monitoring Pt2	1.6 Behavioral, Contextual ID, and Biometrics	Advanced ZT	11.2	DoD Organizations 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 and Just-Enough-Access solution.	UEBA/Entity Monitoring is integrated with JIT/JEA for all services	User Activity Monitoring Pt1	Real-Time Access Decisions; AI-enabled Dynamic Access Control; Enrich Attributes for Resource Authorization Pt1; AI-enabled Network Access
1.7.1	Deny User by Default Policy	1.7 Least Privileged Access	Target Level ZT	22.7	DoD Organizations audit internal user and group usage for permissions and revoke permissions when possible. 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 reduced permissions preparing for future rule/dynamic based access.	Applications updated to deny by default to functions/data requiring specific roles/attributes for access; Reduced default permissions levels are implemented; Applications/services have reviewed/audited all privileged users and removed those users who do not need that level of access; Applications' identify functions and data requiring specific roles/attributes for access		
1.8.1	Single Authentication	1.8 Continuous Authentication	Target Level ZT	19.2	DoD Organizations employ basic authentication processes to authenticate users and NPEs at least once per session (e.g., logon). Importantly users being authenticated are managed by the parallel activity "Organizational MFA/IDP" with the Organizational Identity Provider (IdP) versus using application/service-based identities and groups.	Authentication implemented across applications per session		Periodic Authentication; Rule Based Dynamic Access Pt1
1.8.2	Periodic Authentication	1.8 Continuous Authentication	Target Level ZT	25.4	DoD Organizations enable period authentication requirements for applications and services. Traditionally these are based on duration and/or duration timeout but other period based analytics can be used to mandate re-authentication of user sessions.	Authentication implemented multiple times per session based on security attributes	Single Authentication	Continuous Authentication Pt1; AI-enabled Network Access
1.8.3	Continuous Authentication Pt 1	1.8 Continuous Authentication	Advanced ZT	16.8	DoD Organizations' applications/service utilize multiple session authentications based on security attributes and access requested. Privilege changes and associational transaction requests required additional levels of authentication such as Multi-Factor Authentication (MFA) pushes to users.	Transaction authentication implemented per session based on security attributes	Periodic Authentication	Continuous Authentication Pt2
1.8.4	Continuous Authentication Pt 2	1.8 Continuous Authentication	Advanced ZT	16.8	DoD Organizations continue usage of transaction-based authentication to include integration such as user patterns.	Transaction authentication implemented per session based on security attributes	Continuous Authentication Pt1	Real-Time Access Decisions; AI-enabled Dynamic Access Control
1.9.1	Enterprise PKI/IDP Pt1	1.9 Integrated ICAM Platform	Target Level ZT	12.4	The DoD Enterprise works with Organizations to implement Enterprise Public Key Infrastructure (PKI) and Identity Provider (IdP) solutions in a centralized and/or federated fashion. The Enterprise PKI solution utilizes a single or set of Enterprise level Root Certificate Authorities (CA) which can then be trusted by Organizations to build Intermediate CA's off. The Identity Provider solution may either be a single solution or federated set of Organizational IdPs with standard level of access across Organizations and standardized set of attributes. Organizations' IdPs and PKI Certificated Authorities are integrated with the Enterprise IdP and PKI solutions.	Components are using IdP with MFA for all applications/services; Organizational MFA/PKI integrated with Enterprise MFA/PKI; Organizational Standardized PKI for all services		Enterprise PKI/IDP Pt2
1.9.2	Enterprise PKI/IDP Pt2	1.9 Integrated ICAM Platform	Advanced ZT	27.2	DoD Organizations enable Biometric support in the Identity Provider (IdP) for mission/task-critical applications and services as appropriate. Biometric functionality is moved from Organizational solutions to the Enterprise. Organizational Multi-Factor (MFA) and Public Key Infrastructure (PKI) is decommissioned and migrated to the Enterprise as appropriate.	Critical Organizational Services Integrated w/ Biometrics; Decommission organizational MFA/PKI as appropriate in leu of enterprise MFA/PKI; Enterprise Biometric Functions Implemented	Enterprise PKI/IDP Pt1	Enterprise PKI/IDP Pt3
1.9.3	Enterprise PKI/IDP Pt3	1.9 Integrated ICAM Platform	Advanced ZT	30.0	DoD Organizations integrate the remaining applications/services with Biometrics functionalities. Alternative Multi-Factor (MFA) tokens can be used.	All Organizational Services Integrate w/ Biometrics	Enterprise PKI/IDP Pt2	
2.1.1	Device Health Tool Gap Analysis	2.1 Device Inventory	Target Level ZT	9.8	DoD Organizations develop a manual inventory of devices within the environment. Device attributes tracked in the inventory enable functionality outlined in the ZTA target level.	Manual inventory of devices is created per organization w/ owners		

DoD Zero Trust Activities

ID#	Activity Name	Associated Capability	Phase	Duration (months)	Descriptions	Outcomes	Predecessor(s)	Successor(s)
2.1.2	NPE/PKI, Device under Management	2.1 Device Inventory	Target Level ZT	22.8	DoD Organizations utilize the DoD Enterprise PKI solution/service to deploy x509 certificates to all supported and managed devices. Additional other Non-Person Entities (NPEs) that support x509 certificates are assigned in the PKI and/or IdP systems.	Non-person entities are managed via Org PKI and Org IDP	Enterprise Device Management Pt1	Implement C2C/Compliance Based Network Authorization Pt1; Enterprise PKI Pt1; Deny Device by Default Policy
2.1.3	Enterprise IDP Pt1	2.1 Device Inventory	Target Level ZT	12.8	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.	NPEs including devices are integrated with Enterprise IDP		Enterprise IDP Pt2
2.1.4	Enterprise IDP Pt2	2.1 Device Inventory	Advanced ZT	8.8	The DoD Enterprise Identity Provider (IdP) either using a centralized technology or federated organizational technologies adds additional dynamic attributes for NPEs such as location, usage patterns, etc.	Conditional device attributes are part of the IdP profile	Enterprise IDP Pt1	
2.2.1	Implement C2C/Compliance Based Network Authorization Pt1	2.2 Device Detection and Compliance	Target Level ZT	9.4	The DoD Enterprise working with the Organizations develops a policy, standard and requirements for Comply to Connect. Once agreement is reached solution procurement is started, a vendor(s) is selected, and implementation begins with base level functionality in ZT Target environments (low risk). Base level checks are implemented in the new Comply to Connection solution enabling the ability to meet ZTA target functionalities.	C2C is enforced at the enterprise level for low risk and testing environments; Basic devices checks are implemented using C2C	NPE/PKI Device Under Management; Integrate NextGen AV Tools with C2C; Managed and Limited BYOD & IOT Support; Implement Asset, Vulnerability and Patch Management Tools	Implement C2C/Compliance Based Network Authorization Pt2
2.2.2	Implement C2C/Compliance Based Network Authorization Pt2	2.2 Device Detection and Compliance	Advanced ZT	18.2	DoD Organizations expand the deployment and usage of Comply to Connect to all supported environments required to meet ZT advanced functionalities. Comply to Connect teams integrate their solution(s) with the Enterprise IdP and Authorization Gateways to better manage access and authorizations to resources.	C2C is enforced in all supported environments; Advanced devices checks are completed and integrated with dynamic access (Enterprise IDP / ZTNA)	Implement C2C/Compliance Based Network Authorization Pt1; Fully Integrate Device Security Stack w/ C2C as appropriate	Real-Time Access Decisions
2.3.1	Entity Activity Monitoring Pt1	2.3 Device Authorization w/ Real Time Inspection	Advanced ZT	16.4	Using the developed User and Device baselines, DoD Organizations 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 detections.	UEBA attributes are integrated for device baselining; UEBA attributes are available for usage with device access	User/Device Baselines; Implement User & Entity Behavior Activity (UEBA); User Activity Monitoring Tooling	Entity Activity Monitoring Pt2
2.3.2	Entity Activity Monitoring Pt2	2.3 Device Authorization w/ Real Time Inspection	Advanced ZT	16.7	DoD Organizations 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.	UEBA attributes are mandated for device access	Entity Activity Monitoring Pt1	Real-Time Access Decisions; AI-enabled Dynamic Access Control; Enrich Attributes for Resource Authorization Pt1; AI-enabled Network Access
2.3.3	Implement Application Control & File Integrity Monitoring (FIM) Tools	2.3 Device Authorization w/ Real Time Inspection	Target Level ZT	16.2	DoD Organizations procure and implement File Integrity Monitoring (FIM) and Application Control solutions. FIM continues development and expansion of monitoring in the Data Pillar. Application Control is deployed to low-risk environments in a monitor only mode establishing baseline allowances. Application control teams being integration with the Enterprise and Organization PKI environments utilize certificates for application allowances. NextGen AV covers all possible services and applications.	AppControl and FIM tooling is implemented on all critical services/applications; EDR tooling covers maximum amount of services/applications; AppControl and FIM data is sent to C2C as needed		
2.3.4	Integrate NextGen AV Tools with C2C	2.3 Device Authorization w/ Real Time Inspection	Target Level ZT	18.5	DoD Organizations procure and implement Next Generation Anti-Virus & Anti-Malware solutions as needed. These solutions are integrated with the initial deployment of Comply to Connect for baseline status checks of signatures, updates, etc.	Critical NextGen AV data is being sent to C2C for checks; NextGen AV tooling is implemented on all critical services/applications		Implement C2C/Compliance Based Network Authorization Pt1
2.3.5	Fully Integrate Device Security stack with C2C as appropriate	2.3 Device Authorization w/ Real Time Inspection	Advanced ZT	13.3	DoD Organizations 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 for expanded access decision making data points. Comply to Connect analytics are evaluated for further device/endpoint security stack data points such as UEDM and are integrated as necessary.	AppControl and FIM deployment is expanded to all necessary services/applications; Remaining data from Device Security tooling is implemented with C2C		Implement C2C/Compliance Based Network Authorization Pt2; Managed and Full BYOD & IOT Support Pt2

ID#	Activity Name	Associated Capability	Phase	Duration (months)	Descriptions	Outcomes	Predecessor(s)	Successor(s)
2.3.6	Enterprise PKI Pt1	2.3 Device Authorization w/ Real Time Inspection	Advanced ZT	22.7	The DoD Enterprise Public Key Infrastructure (PKI) is expanded to include the addition of NPE and device certificates. NPEs and device that do not support PKI certificates are marked for retirement and decommission starts.	Devices that are unable to have certificates are phased out and/or moved to minimal access environments; All devices and NPEs have certs installed for authentication in the Enterprise PKI	Implement UEDM or equivalent Tools; NPE/PKI Device Under Management	Enterprise PKI Pt2
2.3.7	Enterprise PKI Pt2	2.3 Device Authorization w/ Real Time Inspection	Advanced ZT	10.5	DoD Organizations utilize certificates for device authentication and machine to machine communications. Unsupported devices complete retirement and exceptions are approved using a risk based methodical approach.	Devices are required to authenticate to communicate with other services and devices	Enterprise PKI Pt1	
2.4.1	Deny Device by Default Policy	2.4 Remote Access	Target Level ZT	9.6	DoD Organizations block all unmanaged remote and local device access to resources. Compliant managed devices are provided risk based methodical access following ZTA target level concepts.	Components can block device access by default to resources (apps/data) and explicitly allow compliant devices per policy; Remote Access is enabled following a "deny device by default policy" approach	NPE/PKI Device Under Management	
2.4.2	Managed and Limited BYOD & IOT Support	2.4 Remote Access	Target Level ZT	39.7	DoD Organizations utilize Unified Endpoint and Device Management (UEDM) and similar solutions to ensure that managed Bring Your Own Device (BYOD) and Internet of Things (IoT) devices are fully integrated with Enterprise IdP enable user and device-based authorization are supported. Device access for all applications requires dynamic access policies.	All applications require dynamic permissions access for devices; BYOD and IOT device permissions are baselined and integrated with Enterprise IDP		Implement C2C/Compliance Based Network Authorization Pt1; Managed and Full BYOD & IOT Support Pt1
2.4.3	Managed and Full BYOD & IOT Support Pt1	2.4 Remote Access	Advanced ZT	24.7	DoD Organizations 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.	Only BYOD and IOT devices that meet mandated configuration standards allowed to access resources; Critical Services require dynamic access for devices	Managed and Limited BYOD & IOT Support	Managed and Full BYOD & IOT Support Pt2
2.4.4	Managed and Full BYOD & IOT Support Pt2	2.4 Remote Access	Advanced ZT	24.6	DoD Organizations utilize Unified Endpoint and Device Management (UEDM) and similar solutions to enable access for unmanaged devices meeting device checks and standard baselines. All possible services/applications are integrated to allow access to managed devices. Unmanaged devices are integrated with services/applications based on risk driven methodical authorization approach.	All possible services require dynamic access for devices	Fully Integrate Device Security Stack w/ C2C as appropriate; Managed and Full BYOD & IOT Support Pt1	
2.5.1	Implement Asset, Vulnerability and Patch Management Tools	2.5 Partially & Fully Automated Asset, Vulnerability and Patch Management	Target Level ZT	18.4	DoD Organizations implement solution(s) for managing assets/devices configurations, vulnerabilities, and patches. Using minimum compliance standards (e.g., STIGs, 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.	Components can confirm if devices meet minimum compliance standards or not; Components have asset management, vulnerability, and patching systems with APIs that will enable integration across the systems		Implement C2C/Compliance Based Network Authorization Pt1
2.6.1	Implement UEDM or equivalent Tools	2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM)	Target Level ZT	18.1	DoD Organizations will work closely with the “Implement Asset, Vulnerability, and Patch Management tools” activity to procure and implement and Unified Endpoint and 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 functionalities such as minimum compliance, asset management, and API support are in place.	Components can confirm if devices meet minimum compliance standards or not; Components have asset management system(s) for user devices (phones, desktops, laptops) that maintains IT compliance, which is reported up to DoD enterprise; Components asset management systems can programmatically, i.e., API, provide device compliance status and if it meets minimum standards		Enterprise PKI Pt1
2.6.2	Enterprise Device Management Pt1	2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM)	Target Level ZT	17.6	DoD Organizations migrate the manual device inventory to an automated approach using the Unified Endpoint and Device Management solution. Approved devices are able to be managed regardless of location. Devices part of critical services are mandated to be managed by the Unified Endpoint and Device Management solution supporting automation.	Manual inventory is integrated with an automated management solution for critical services; Enable ZT Device Management (from any location with or without remote access)		NPE/PKI Device Under Management; Enterprise Device Management Pt2
2.6.3	Enterprise Device Management Pt2	2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM)	Target Level ZT	12.6	DoD Organizations migrate the remaining devices to Enterprise Device Management solution. EDM solution is integrated with risk and compliance solutions as appropriate.	Manual inventory is integrated with an automated management solution for all services	Enterprise Device Management Pt1	
2.7.1	Implement Endpoint Detection & Response (EDR) Tools and Integrate with C2C	2.7 Endpoint & Extended Detection & Response (EDR & XDR)	Target Level ZT	16.5	DoD Organizations 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 functionality and is sending data to the Comply to Connection solution for expanded device and user checks.	Endpoint Detection & Response Tooling is implemented ; Critical EDR data is being sent to C2C for checks; NextGen AV tooling covers maximum amount of services/applications		Implement Extended Detection & Response (XDR) & Integrate w/ C2C Pt 1

DoD Zero Trust Activities

ID#	Activity Name	Associated Capability	Phase	Duration (months)	Descriptions	Outcomes	Predecessor(s)	Successor(s)
2.7.2	Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt1	2.7 Endpoint & Extended Detection & Response (EDR & XDR)	Target Level ZT	19.2	DoD Organizations procure and implement Extended Detection & Response (XDR) solution(s). Integration points with cross pillar capabilities are identified and prioritized based on risk. The riskiest of these integration points are actioned and integration is started. EDR continues coverage of endpoints to include the maximum number of services and applications as part of the XDR implementation. Basic analytics are sent from the XDR solution stack to the SIEM.	Integration Points have been identified per Capability; Riskiest integration points have been integrated w/ XDR; Basic alerting is in place with SIEM and/or other mechanisms	Implement Endpoint Detection & Response (EDR) Tools & Integrate w/ C2C; Threat Alerting Pt1	Implement Extended Detection & Response (XDR) & Integrate w/ C2C Pt 2
2.7.3	Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt2	2.7 Endpoint & Extended Detection & Response (EDR & XDR)	Advanced ZT	19.9	XDR solution stack completes identification of integration points expanding coverage to the fullest amount possible. Exceptions are tracked and managed using a risk based methodical approach for continued operation. Extended analytics enabling ZT Advanced functionalities are integrated into the SIEM and other appropriate solutions.	Remaining integration points have been integrate as appropriate; Extended alerting and response is enabled with other Analytics tools at least using SIEM	Implement Extended Detection & Response (XDR) & Integrate w/ C2C Pt 1	Threat Alerting Pt3
3.1.1	Application/Code Identification	3.1 Application Inventory	Target Level ZT	16.7	DoD Organizations create an inventory of approved applications and code (e.g., source code, libraries, etc.). Each organization will track the supportability (i.e., active, legacy, etc.) and hosted location (i.e., cloud, on-premise, hybrid, etc.) at least in the inventory.	Component has identified applications and classified as either legacy, virtualized on-premises, and cloud hosted		
3.2.1	Build DevSecOps Software Factory Pt1	3.2 Secure Software Development & Integration	Target Level ZT	19.3	The DoD enterprise creates the foundational standards for modern DevSecOps processes and CI/CD pipelines. The concepts are applied in a standardized technology stack across DoD organizations able to meet future Application Security requirements. An enterprise-wide Vulnerability Management program is integrated with the CI/CD pipelines following the Vulnerability Management Program activities.	Developed Data/Service Standards for DevSecOps; CI/CD Pipeline is fully functional and tested successfully; Vulnerability Management program is officially in place and operating		Build DevSecOps Software Factory Pt2
3.2.2	Build DevSecOps Software Factory Pt2	3.2 Secure Software Development & Integration	Target Level ZT	10.8	DoD Organizations will 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.	Development of applications is migrated to CI/CD pipeline; Continual validation process/technology is implemented and in use; Development of applications is migrated to DevSecOps process and technology	Build DevSecOps Software Factory Pt1	Continuous Authorization to Operate (cATO) Pt1
3.2.3	Automate Application Security & Code Remediation Pt1	3.2 Secure Software Development & Integration	**Target Level ZT**	18.0	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 a Secure API gateway 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 appropriate.	Secure API Gateway is operational and majority of API calls are passing through gateway; Application Security functions (e.g., code review, container and serverless security) are implemented as part of CI/CD and DevSecOps	Implement Asset, Vulnerability and Patch Management Tools	Automate Application Security & Code Remediation Pt2; REST API Micro-Segments
3.2.4	Automate Application Security & Code Remediation Pt2	3.2 Secure Software Development & Integration	Advanced ZT	16.2	DoD Organizations modernize approaches to delivering internally developed and managed services following best practice approaches such as Microservices. These approaches will enable more resilient and secure architectures by allowing for quicker changes to code in each microservice as security issues are discovered. Further advancement security remediation activities continue across the DoD Enterprise with the inclusion of runtime security functions for containers as appropriate, automated vulnerable library updates and automated CI/CD approvals during the release process.	Secure API Gateway is operational and majority of API calls are passing through gateway; Services are provided following a Service Oriented Architecture (SOA); Security Remediation activities (e.g., runtime security, library updates, release approvals) are fully automated	Automate Application Security & Code Remediation Pt1	
3.3.1	Approved Binaries/Code	3.3 Software Risk Management	Target Level ZT	23.4	The DoD enterprise uses best practice approaches to manage approved binaries and code in a methodical approach. These approaches will include supplier sourcing risk management, approved repository usage, bill of materials supply chain risk management, and industry standard vulnerability management.	Supplier sourcing risk evaluated and identified for approved sources; Repository and update channel established for use by development teams; Bill of Materials is created for applications identify source, supportability and risk posture; Industry standard (DIB) and approved vulnerability databases are pulled in to be used in DevSecOps	Vulnerability Management Program Pt1	

ID#	Activity Name	Associated Capability	Phase	Duration (months)	Descriptions	Outcomes	Predecessor(s)	Successor(s)
3.3.2	Vulnerability Management Program Pt1	3.3 Software Risk Management	Target Level ZT	7.8	The DoD Enterprise works with Organizations to establish and manage a Vulnerability Management program. The program includes a policy and standards agreed upon by all Organizations. The developed program includes at a minimum the track and management of public vulnerabilities based on DoD applications/services. Organizations establish a vulnerability management team with key stakeholders where vulnerabilities are discussed and managed following the Enterprise policy and standards.	Vulnerability Management Team is in place w/ appropriate stakeholder membership; Vulnerability Management policy and process is in place and agreed to w/ stakeholders; Public source of vulnerabilities are being utilized for tracking		Approved Binaries/Code; Vulnerability Management Program Pt2
3.3.3	Vulnerability Management Program Pt2	3.3 Software Risk Management	Target Level ZT	12.1	Processes are established at the DoD Enterprise level for managing the disclosure of vulnerabilities in DoD maintained/operated services both publicly and privately accessible. DoD Organizations expand the vulnerability management program to track and manage closed vulnerability repositories such as DIB, CERT, and others.	Controlled (e.g., DIB, CERT) sources of vulnerabilities are being utilized for tracking; Vulnerability management program has a process for accepting external/public disclosures for managed services	Vulnerability Management Program Pt1	Automate Application Security & Code Remediation Pt1
3.3.4	Continual Validation	3.3 Software Risk Management	Target Level ZT	11.1	DoD Organizations will implement a continual validation approach for application development where parallel deployment is conducted and integrated with an approved environment level (e.g., UAT, Prod). Applications unable to integrate continual validation into their CI/CD process are identified and exceptions are provided as needed using a methodical approach.	Updated Applications are deployed in a live and/or production environment; Applications that were marked for retirement and transition are decommissioned; Continual validation tools are implemented and applied to code in the CI/CD pipeline; Code requiring continuous validation is identified and validation criteria are established		
3.4.1	Resource Authorization Pt1	3.4 Resource Authorization & Integration	Target Level ZT	18.5	The DoD Enterprise standardizes on resource authorization approaches (e.g., Software Defined Perimeter) with the organizations. At a minimum the resource authorization gateways will be integrated with identities and devices. Organizations deploy approved resource authorization gateways and enable for external facing applications/services. Additional applications for migration and applications unable to be migrated are identified for exception or decommission.	Resource Authorization Gateway is in place for external facing applications; Resource Authorization policy integrated with identity and device; Enterprise-wide Guidance on conversion standards are communicated to stakeholders	NPE/PKI, Device under Management Datacenter Macro segmentation	Resource Authorization Pt2
3.4.2	Resource Authorization Pt2	3.4 Resource Authorization & Integration	Target Level ZT	20.6	Resource authorization gateways are used for all possible applications/services. Application unable to utilize gateways are either decommissioned or excepted using a risk based methodical approach. Authorizations are further integrated with the CI/CD pipeline for automated decision making.	Resource Authorization gateway is utilized for all applications; Resource Authorization is integrated with DevSecOps and CI/CD for automated functions	Resource Authorization Pt1	
3.4.3	SDC Resource Authorization Pt1	3.4 Resource Authorization & Integration	Target Level ZT	31.1	The DoD Enterprise provides a standardized approach for code based compute management (i.e., Software Defined Compute) following industry best practices. Using risk-based approaches baselines are created using the approved set of code libraires and packages. DoD Organizations work with the approved code/binaries activities to ensure that applications are identified which can and cannot support the approach. Applications which can support a modern software-based configuration and management approaches are identified and transitioning begins. Applications which cannot follow software-based configuration and management approaches are identified and allowed through exception using a methodical approach.	Applications unable to be updated to use approved binaries/code are marked for retirement and transition plans are created; Identified applications without approved binaries and code are updated to use approved binaries/code; Enterprise-wide Guidance on conversion standards are communicated to stakeholders		SDC Resource Authorization Pt2
3.4.4	SDC Resource Authorization Pt2	3.4 Resource Authorization & Integration	Target Level ZT	21.8	Applications which support software-based configuration and management have been transitioned to a production/live environment and are in normal operations. Where possible applications which cannot support software-based configuration and management are decommissioned.	Updated Applications are deployed in a live and/or production environment; Applications that were marked for retirement and transition are decommissioned	SDC Resource Authorization Pt1	
3.4.5	Enrich Attributes for Resource Authorization Pt1	3.4 Resource Authorization & Integration	Advanced ZT	17.6	Initial attributes from sources such as User and Entity Activity Monitoring, Micro-segmentation services, DLP and DRM are integrated into the Resource Authorization technology stack and policy. 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.	Most API calls are passing through the Secure API Gateway; Resource Authorization receives data from Analytics Engine; Authorization policies incorporate identified attributes in making authorization decisions; Attributes to be used for initial enrichment are identified; Identified attributes are assigned to resources and/or entities	User Activity Monitoring Pt2; Entity Activity Monitoring Pt2; Application & Device Micro segmentation; Manual Data Tagging Pt2; DLP Enforcement via Data Tags and Analytics Pt2; DRM Enforcement via Data Tags and Analytics Pt2	Enrich Attributes for Resource Authorization Pt2

ID#	Activity Name	Associated Capability	Phase	Duration (months)	Descriptions	Outcomes	Predecessor(s)	Successor(s)
3.4.6	Enrich Attributes for Resource Authorization Pt2	3.4 Resource Authorization & Integration	Advanced ZT	17.8	Extended identified attributes are integrated with the resource authorization technology and policy. Confidence scoring is introduced across the attributes to create a more advanced method of authorization decision making in an automated fashion.	Authorization policies incorporate confidence levels in making authorization decisions; Confidence levels for attributes are defined	Enrich Attributes for Resource Authorization Pt1	
3.4.7	REST API Micro-Segments	3.4 Resource Authorization & Integration	Advanced ZT	18.1	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 Controllers and/or Software Defined Networking Consoles.	Approved Enterprise APIs are Micro-Segmented appropriately	Automate Application Security & Code Remediation Pt1	
3.5.1	Continuous Authorization to Operate (cATO) Pt1	3.5 Continuous Monitoring and Ongoing Authorizations	Advanced ZT	15.1	DoD Organizations 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.	Controls derivation is standardized and ready for automation; Controls testing is integrated with DevSecOps processes and technology	Policy Inventory & Development; Build DevSecOps Software Factory Pt2	Continuous Authorization to Operate (ATO) Pt2
3.5.2	Continuous Authorization to Operate (cATO) Pt2	3.5 Continuous Monitoring and Ongoing Authorizations	Advanced ZT	21.8	DoD Organizations fully automate control derivation, testing and monitoring processes. Deviations are automatically tested and resolved using existing cross pillar automation infrastructure. Dashboarding is used to monitor the status of authorizations and analytics are integrated with the responsible authorizing officials.	Controls testing is fully automated; Integration with standard IR and SOC operations is automated; Control derivation and applicability is fully automated; Dashboards are used to track continuing authorization status	Continuous Authorization to Operate (ATO) Pt1; Threat Alerting Pt3; Automated Workflow	
4.1.1	Data Analysis	4.1 Data Catalog Risk Alignment	Target Level ZT	17.4	DoD Organizations update the service and application catalog(s) with data classifications. Data tags are also added to each service and application.	The service catalog is updated with data types for each application and service based on data classification levels		
4.2.1	Define Data Tagging Standards	4.2 DoD Enterprise Data Governance	Target Level ZT	15.8	The DoD Enterprise works with organizations 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.	Enterprise data classification and tagging standards are developed; Organizations align to enterprise standards and begin implementation		Implement Data Tagging & Classification Tools; Manual Data Tagging Pt1
4.2.2	Interoperability Standards	4.2 DoD Enterprise Data Governance	Target Level ZT	14.4	The DoD Enterprise collaborating with the organizations develops interoperability standards integrating mandatory Data Rights Management (DRM) and Protection solutions with necessary technologies to enable ZT target functionality.	Formal standards are in place by the Enterprise for the appropriate data standards		Implement DRM and Protection Tools Pt1
4.2.3	Develop Software Defined Storage (SDS) Policy	4.2 DoD Enterprise Data Governance	Target Level ZT	9.9	The DoD enterprise working with organizations establishes a software define storage (SDS) policy and standards based on industry best practices. DoD organizations evaluate current data storage strategy and technology for implementation of SDS. Where appropriate storage technology is identified for SDS implementation.	Determine need for SDS tool implementation; Policy for SDS is created at the enterprise and org levels		Integrate DAAS Access w/ SDS Policy Pt1; Integrate Solution & Policy w/ Enterprise IDP Pt1
4.3.1	Implement Data Tagging & Classification Tools	4.3 Data Labeling and Tagging	Target Level ZT	15.9	DoD Organizations utilize the enterprise standard and requirements to implement data tagging and classification solution(s). Organizations ensure that future ML and AI integrations are supported by solutions through DoD enterprise requirements.	A requirement of Data classification and tagging tools must include integration and/or support of Machine Learning (ML); Data classification and tagging tools are implemented at org and enterprise levels	Define Data Tagging Standards	Implement Enforcement Points
4.3.2	Manual Data Tagging Pt1	4.3 Data Labeling and Tagging	Target Level ZT	17.6	Using the DoD Enterprise data tagging and classification policy and standards, manual tagging starts using basic data level attributes to meet ZT target functionality.	Manual data tagging begins at the enterprise level with basic attributes	Define Data Tagging Standards	Manual Data Tagging Pt2; DRM Enforcement via Data Tags and Analytics Pt1; DLP Enforcement via Data Tags and Analytics Pt1
4.3.3	Manual Data Tagging Pt2	4.3 Data Labeling and Tagging	Advanced ZT	16.1	DoD organizational specific data level attributes are integrated into the manual data tagging process. DoD enterprise and organizations collaborate to decide which attributes are required to meet ZTA advanced functionality. Data level attributes for ZTA advanced functionality are standardized across the enterprise and incorporated.	Manual data tagging is expanded to the program/org levels with specific attributes	Manual Data Tagging Pt1	Enrich Attributes for Resource Authorization Pt1
4.3.4	Automated Data Tagging & Support Pt1	4.3 Data Labeling and Tagging	Advanced ZT	14.1	DoD Organizations use data loss prevention, rights management, 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.	Basic automation begins by scanning data repositories and applying tags	Implement Data Tagging & Classification ML Tools	Automated Data Tagging & Support Pt2

ID#	Activity Name	Associated Capability	Phase	Duration (months)	Descriptions	Outcomes	Predecessor(s)	Successor(s)
4.3.5	Automated Data Tagging & Support Pt2	4.3 Data Labeling and Tagging	Advanced ZT	38.8	Remaining supported data repositories have basic and extended data tags which are applied using machine learning and artificial intelligence. 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.	Full automation of data tagging is completed; Results of data tagging are fed into ML algorithms to develop AI driven data tagging	Automated Data Tagging & Support Pt1	
4.4.1	DLP Enforcement Point Logging and Analysis	4.4 Data Monitoring and Sensing	Target Level ZT	10.8	DoD Organizations identify data loss prevention (DLP) enforcement points such as specific services and user endpoints. Using the established DoD Enterprise cybersecurity incident response standard, DoD organizations ensure the appropriate detail of data is captured. Additionally, protection, detection, and response use cases are developed to better outline solution coverage.	Enforcement points are identified; Standardized Logging schema is enforced at the enterprise and org levels		Comprehensive Data Activity Monitoring
4.4.2	DRM Enforcement Point Logging and Analysis	4.4 Data Monitoring and Sensing	Target Level ZT	12.6	DoD Organizations identify data rights management (DRM) enforcement points such as specific services and user endpoints. Using the established DoD Enterprise cybersecurity incident response standard, DoD organizations ensure the appropriate detail of data is captured. Additionally, protection, detection, and response use cases are developed to better outline solution coverage.	Enforcement points are identified; Standardized Logging schema is enforced at the enterprise and org levels		Comprehensive Data Activity Monitoring
4.4.3	File Activity Monitoring Pt1	4.4 Data Monitoring and Sensing	Target Level ZT	16.8	DoD Organizations 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 functionality.	Data and files of critical classification are actively being monitored; Basic Integration is in place with monitoring system such as the SIEM		File Activity Monitoring Pt2
4.4.4	File Activity Monitoring Pt2	4.4 Data Monitoring and Sensing	Target Level ZT	18.9	DoD Organizations 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.	Data and files of all regulated classifications are actively being monitored; Extended integrations are in place as appropriate to further manage risk	File Activity Monitoring Pt1	Rule Based Dynamic Access Pt2; Database Activity Monitoring
4.4.5	Database Activity Monitoring	4.4 Data Monitoring and Sensing	Advanced ZT	18.2	DoD Organizations procure, implement, and utilize Database Monitor solutions to monitor all databases containing regulated data types (CUI, PII, PHI, etc.). Logs and analytics from the database monitoring solution are fed to the SIEM for monitoring and response. Analytics are fed into cross pillar activities such as "Enterprise Security Profile" and "Real Time Access" to better direct decision making.	Appropriate Database are being actively monitored; Monitoring technology is integrated with solutions such as SIEM, PDP and Dynamic Access Control mechanisms	File Activity Monitoring Pt2	Comprehensive Data Activity Monitoring
4.4.6	Comprehensive Data Activity Monitoring	4.4 Data Monitoring and Sensing	Advanced ZT	27.2	DoD Organizations expand monitoring of data repositories including databases as appropriate based on a methodical risk approach. Additional data attributes to meet the ZT Advanced functionalities are integrated into the analytics for additional integrations.	Data Activity monitoring mechanisms are integrated to provide a unified view of monitoring across data repositories; Appropriate integrations exist with solutions such as SIEM and PDP	DLP Enforcement Point Logging and Analysis; DRM Enforcement Point Logging and Analysis; Database Activity Monitoring	AI-enabled Dynamic Access Control; FF Baseline & Profiling Pt. 2; AI-enabled Network Access
4.5.1	Implement DRM and Protection Tools Pt1	4.5 Data Encryption & Rights Management	Target Level ZT	11.7	DoD Organizations 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 implemented with high risk data repositories using ZTA target level protections.	DRM and protection tools are enabled for high risk data repositories with basic protections	Interoperability Standards	Implement DRM and Protection Tools Pt2
4.5.2	Implement DRM and Protection Tools Pt2	4.5 Data Encryption & Rights Management	Target Level ZT	22.0	DRM and protection coverage is expanded to cover all in scope data repositories. Encryption keys are automatically managed to meet best practices (e.g., FIPS). Extended data protection attributes are implemented based on the environment classification.	DRM and protection tools are enabled for possible repositories	Implement DRM and Protection Tools Pt1	
4.5.3	DRM Enforcement via Data Tags and Analytics Pt1	4.5 Data Encryption & Rights Management	Target Level ZT	16.2	Data rights management (DRM) and protection solutions are integrated with basic data tags defined by the DoD Enterprise standard. Initial data repositories are monitored and have protect and response actions enabled. Data at rest is encrypted in repositories.	Data Tags are integrated with DRM and monitored repositories are expanded; Based on data tags, data is encrypted at rest	Manual Data Tagging Pt1	DRM Enforcement via Data Tags and Analytics Pt2

DoD Zero Trust Activities

ID#	Activity Name	Associated Capability	Phase	Duration (months)	Descriptions	Outcomes	Predecessor(s)	Successor(s)
4.5.4	DRM Enforcement via Data Tags and Analytics Pt2	4.5 Data Encryption & Rights Management	Advanced ZT	19.0	Extended data repositories are protected with DRM and Protection solutions. DoD Organizations implement extended data tags applicable to organizations versus mandated enterprise. Data is encrypted in extended repositories using additional tags.	All applicable data repositories are protected using DRM; Data is encrypted using extended data tags from the org levels	DRM Enforcement via Data Tags and Analytics Pt1	Enrich Attributes for Resource Authorization Pt1; DRM Enforcement via Data Tags and Analytics Pt3
4.5.5	DRM Enforcement via Data Tags and Analytics Pt3	4.5 Data Encryption & Rights Management	Advanced ZT	23.3	DRM and Protection solutions integrate with AI and ML tooling for encryption, rights management and protection functions.	Analytics from ML/AI are integrated with DRM to better automate protections; Encryption protection is integrated with AI/ML and updated encryption methods are used as needed	DRM Enforcement via Data Tags and Analytics Pt2	
4.6.1	Implement Enforcement Points	4.6 Data Loss Prevention (DLP)	Target Level ZT	21.2	Data loss prevention (DLP) solution is deployed to the in-scope enforcement points. DLP solution is set to "monitor-only" and/or "learning" mode limiting impact. DLP solution results are analyzed, and policy is fine tuned to manage risk to an acceptable level.	Identified enforcement points have DLP tool deployed and set to monitor mode with standardized logging	Implement Data Tagging & Classification Tools	Process Micro segmentation
4.6.2	DLP Enforcement via Data Tags and Analytics Pt1	4.6 Data Loss Prevention (DLP)	Target Level ZT	21.3	Data loss prevention (DLP) solution is updated from monitor only mode to prevention mode. Basic data tags are utilized for DLP solution and logging schema is integrated.	Enforcement Points to set to prevent mode integrating the logging schema and manual tags	Manual Data Tagging Pt1	DLP Enforcement via Data Tags and Analytics Pt2
4.6.3	DLP Enforcement via Data Tags and Analytics Pt2	4.6 Data Loss Prevention (DLP)	Advanced ZT	19.0	Data loss prevention (DLP) solution is updated to include extended data tags based on parallel Automation activities.	Enforcement points have extended data tag attributes applied for additional prevention	DLP Enforcement via Data Tags and Analytics Pt1	Enrich Attributes for Resource Authorization Pt1; DLP Enforcement via Data Tags and Analytics Pt3
4.6.4	DLP Enforcement via Data Tags and Analytics Pt3	4.6 Data Loss Prevention (DLP)	Advanced ZT	41.6	Data loss prevention (DLP) solution is integrated with automated data tagging techniques to include any missing enforcement points and tags.	Automated tagging attributes are integrated with DLP and resulting metrics are used for ML	DLP Enforcement via Data Tags and Analytics Pt2	
4.7.1	Integrate DAAS Access w/ SDS Policy Pt1	4.7 Data Access Control	Target Level ZT	15.3	Utilizing the DoD enterprise SDS policy, organizational DAAS policy is developed with intended integration in mind. SDS implementation guide is developed by DoD organizations due to environment specific nature.	Attribute base fine-grained DAAS policy is developed w/ enterprise and org level support; SDS Integration plan is developed to support DAAS policy	Develop Software Defined Storage (SDS) Policy	Integrate DAAS Access w/ SDS Policy Pt2
4.7.2	Integrate DAAS Access w/ SDS Policy Pt2	4.7 Data Access Control	Advanced ZT	12.6	DoD Organizations implement the DAAS policy in an automated fashion.	Attribute based fine-grained DAAS Policy implemented in an automated fashion	Integrate DAAS Access w/ SDS Policy Pt1; Implement SDS Tool and/or Integrate w/ DRM Tool Pt1	Integrate DAAS Access w/ SDS Policy Pt3
4.7.3	Integrate DAAS Access w/ SDS Policy Pt3	4.7 Data Access Control	Advanced ZT	9.2	Newly implemented SDS technology and/or functionalities are integrated with the DAAS policy in a risk-based fashion. A phased approach should be taken to during implementation to measure results and adjust accordingly.	SDS is integrated with DAAS policy functionality; all data in all applications are protected with attribute based fine-grained DAAS policy	Integrate DAAS Access w/ SDS Policy Pt2	
4.7.4	Integrate Solution(s) and Policy with Enterprise IDP Pt1	4.7 Data Access Control	Target Level ZT	13.9	DoD Organizations develop an integration plan using the SDS policy and technology/functionality with the enterprise Identity Provider (IdP) solution.	Integration plan between SDS and authoritative Identity Provider is developed to support existing DAAS access	Develop Software Defined Storage (SDS) Policy; Enterprise IDP Pt1	Integrate Solution & Policy w/ Enterprise IDP Pt2
4.7.5	Integrate Solution(s) and Policy with Enterprise IDP Pt2	4.7 Data Access Control	Advanced ZT	9.2	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 functionalities are required for integration.	Complete integration with Enterprise IDP and SDS toolingto support all attribute based fine-grained DAAS access	Integrate Solution & Policy w/ Enterprise IDP Pt1	
4.7.6	Implement SDS Tool and/or integrate with DRM Tool Pt1	4.7 Data Access Control	Advanced ZT	17.4	Depending on the need for a Software Defined Storage tool, a new solution is implemented or an existing solution is identified meeting the functionality requirements to be integrated with DLP, DRM/Protection, and ML solutions.	If tooling is needed ensure there is supported integrations with DLP, DRM and ML tooling	Develop Software Defined Storage (SDS) Policy; Integrate Solution & Policy w/ Enterprise IDP Pt1	Integrate DAAS Access w/ SDS Policy Pt2; Implement SDS Tool and/or Integrate w/ DRM Tool Pt2
4.7.7	Implement SDS Tool and/or integrate with DRM Tool Pt2	4.7 Data Access Control	Advanced ZT	15.3	DoD Organizations configure the SDS functionality and/or solution to be integrated with the underlying DLP and DRM/Protection infrastructure as appropriate. Lower-level integrations enable more effective protection and response.	Integrate SDS infrastructure with existing DLP and DRM infrastructure	Implement SDS Tool and/or Integrate w/ DRM Tool Pt1	
5.1.1	Define Granular Control Access Rules & Policies Pt1	5.1 Data Flow Mapping	Target Level ZT	10.3	The DoD Enterprise working with the Organizations 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 Organizations will implement these access policies into existing network technologies (e.g., Next Generation Firewalls, Intrusion Prevention Systems, etc.) to improve initial risk levels.	Provide Technical Standards; Develop Concept of Operations; Identify Communities of Interest		Define SDN APIs; Define Granular Control Access Rules & Policies Pt2
5.1.2	Define Granular Control Access Rules & Policies Pt2	5.1 Data Flow Mapping	Target Level ZT	8.0	DoD Organizations utilize data tagging and classification standards to develop data filters for API access to the SDN Infrastructure. API Decision Points are formalized within the SDN architecture and implemented with non-mission/task critical applications and services.	Define Data Tagging Filters for API Infrastructure	Define Granular Control Access Rules & Policies Pt1	

DoD Zero Trust Activities

ID#	Activity Name	Associated Capability	Phase	Duration (months)	Descriptions	Outcomes	Predecessor(s)	Successor(s)
5.2.1	Define SDN APIs	5.2 Software Defined Networking (SDN)	Target Level ZT	8.3	The DoD Enterprise works with the Organizations to define the necessary APIs and other programmatic interfaces to enable Software Defined Networking (SDN) functionalities. These APIs will enable Authentication Decision Point, Application Delivery Control Proxy and Segmentation Gateways automation.	SDN APIs are standardized and implemented; APIs are functional for AuthN Decision Point, App Delivery Control Proxy and Segmentation Gateways	Define Granular Control Access Rules & Policies Pt1	Implement SDN Programable Infrastructure
5.2.2	Implement SDN Programable Infrastructure	5.2 Software Defined Networking (SDN)	Target Level ZT	32.0	Following the API standards, requirements and SDN API functionalities, DoD Organizations will implement Software Defined Networking (SDN) infrastructure to enable automation tasks. Segmentation Gateways and Authentication Decision Points are integrated into the SDN infrastructure along with output logging into a standardized repository (e.g., SIEM, Log Analytics) for monitoring and alerting.	Implemented Application Delivery Control Proxy; Established SIEM Logging Activities; Implemented User Activity Monitoring (UAM); Integrated with Authentication Decision Point; Implemented Segmentation Gateways	Define SDN APIs; Standardized API Calls & Schemas Pt1	
5.2.3	Segment Flows into Control, Management, and Data Planes	5.2 Software Defined Networking (SDN)	Target Level ZT	13.0	Network infrastructure and flows are segmented either physically or logically into control, management, and data planes. Basic 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.	IPv6 Segmentation; Enable Automated NetOps Information Reporting; Ensure Configuration Control Across Enterprise; Integrated with SOAR		B/C/P/S Macro segmentation; Application & Device Micro segmentation
5.2.4	Network Asset Discovery & Optimization	5.2 Software Defined Networking (SDN)	Advanced ZT	30.2	DoD Organizations 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 provide necessary approved access to resources.	Technical Refreshment/Technology Evolution; Provide Optimization/Performance Controls		
5.2.5	Real-Time Access Decisions	5.2 Software Defined Networking (SDN)	Advanced ZT	15.6	SDN Infrastructure utilizes cross Pillar data sources such as User Activity Monitoring, Entity Activity Monitoring, Enterprise Security Profiles and more for real-time access decisions. Machine learning is used to assist decision making based on advanced network analytics (full packet capture, etc.). Policies are consistently implemented across the Enterprise using unified access standards.	Analyze SIEM Logs with Analytics Engine to Provide Real-Time Policy Access Decisions; Support Sending Captured Packets, Data/Network Flows, and other Specific Logs for Analytics; Segment End-to-End Transport Network Flows; Audit Security Policies for Consistency across Enterprise; Protect Data-in-Transit During Coalition Information Sharing	Continuous Authentication Pt2; User Activity Monitoring Pt2; Implement C2C/Compliance Based Network Authorization Pt2; Entity Activity Monitoring Pt2; AI-enabled Network Access; Enterprise Security Profile Pt2	
5.3.1	Datacenter Macro segmentation	5.3 Macro Segmentation	Target Level ZT	17.6	DoD Organizations implement data center focused macro-segmentation using traditional tiered (web, app, db) and/or service-based architectures. Proxy and/or enforcement checks are integrated with the SDN solution(s) based on device attributes and behavior.	Log Actions to SIEM; Establish Proxy/Enforcement Checks of Device Attributes, Behavior, and other Data; Analyze Activities with Analytics Engine		Implement Micro segmentation
5.3.2	B/C/P/S Macro segmentation	5.3 Macro Segmentation	Target Level ZT	18.1	DoD Organizations implement base, camp, post, and station macro-segmentation using logical network zones limiting lateral movement. Proxy and/or enforcement checks are integrated with the SDN solution(s) based on device attributes and behavior.	Establish Proxy/Enforcement Checks of Device Attributes, Behavior, and other Data; Log Actions to SIEM; Analyze Activities with Analytics Engine; Leverage SOAR to Provide RT Policy Access Decisions	Segment Flows into Control, Management, and Data Planes	
5.4.1	Implement Micro segmentation	5.4 Micro Segmentation	Target Level ZT	17.3	DoD Organizations implement Micro-Segmentation infrastructure into SDN 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.	Accept Automated Policy Changes; Implement API Decision Points; Implement NGF/Micro FW/Endpoint Agent in Virtual Hosting Environment	Datacenter Macro segmentation	Application & Device Micro segmentation
5.4.2	Application & Device Micro segmentation	5.4 Micro Segmentation	Target Level ZT	17.9	DoD Organizations utilize Software Defined Networking (SDN) solution(s) to establish infrastructure meeting the ZT Target functionalities – logical network zones, role, attribute and conditional based access control for user and devices, privileged access management services for network resources, and policy-based control on API access.	Assign Role, Attribute, & Condition Based Access Control to User & Devices; Provide Privileged Access Management Services; Limit Access on Per Identity Basis for User & Device; Create Logical Network Zones; Support Policy Control via REST API	Segment Flows into Control, Management, and Data Planes; Implement Micro segmentation	Enrich Attributes for Resource Authorization Pt1
5.4.3	Process Micro segmentation	5.4 Micro Segmentation	Advanced ZT	20.3	DoD Organizations 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.	Segment Host-Level Processes for Security Policies; Support Real-Time Access Decisions and Policy Changes; Support Offload of Logs for Analytics and Automation; Support Dynamic Deployment of Segmentation Policy	Implement Enforcement Points	

DoD Zero Trust Activities

ID#	Activity Name	Associated Capability	Phase	Duration (months)	Descriptions	Outcomes	Predecessor(s)	Successor(s)
5.4.4	Protect Data In Transit	5.4 Micro Segmentation	Target Level ZT	9.1	Based on the data flow mappings and monitoring, policies are enabled by DoD Organizations 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.	Protect Data In Transit During Coalition Information Sharing; Protect Data in Transit Across System High Boundaries; Integrate Data In Transit Protection Across Architecture Components		
6.1.1	Policy Inventory & Development	6.1 Policy Decision Point (PDP) & Policy Orchestration	Target Level ZT	9.8	The DoD Enterprise works with the Organizations to catalog and inventory existing Cyber Security policies and standards. Policies are updated and created in cross pillar activities as needed to meet critical ZT Target functionality.	Policies have been collected in reference to applicable compliance and risk (e.g. RMF, NIST); Policies have been reviewed for missing Pillars and Capabilities per the ZTRA; Missing areas of policies are updated to meet the capabilities per ZTRA		Continuous Authorization to Operate (cATO) Pt1
6.1.2	Organization Access Profile	6.1 Policy Decision Point (PDP) & Policy Orchestration	Target Level ZT	19.4	DoD Organizations develop basic access profiles for mission/task and non-mission/task DAAS access using the data from the User, Data, Network, and device pillars. The DoD Enterprise works with the Organizations to develop an Enterprise Security Profile using the existing Organizational security profiles to create a common access approach to DAAS. A phased approach can be used in organizations to limit risk to mission/task critical DAAS access once the security profile(s) are created.	Organization scoped profile(s) are created to determine access to DAAS using capabilities from User, Data, Network, and Device pillars; Initial enterprise profile access standard is developed for access to DAAS ; When possible the organization profile(s) utilizes enterprise available services in the User, Data, Network and Device pillars; Organization Mission/Task critical profile(s) are created		Enterprise Security Profile Pt1
6.1.3	Enterprise Security Profile Pt1	6.1 Policy Decision Point (PDP) & Policy Orchestration	Target Level ZT	16.0	The Enterprise Security profile covers the User, Data, Network and Device pillars initially. Existing Organizational Security Profiles are integrated for non-mission/task DAAS access following an iterative approach to tuning access.	Enterprise Profile(s) are created to access DAAS using capabilities from User, Data, Network and Device Pillars; Non-mission/task critical organization profile(s) are integrated with the enterprise profile(s) using a standardized approach	Organization Access Profile	Enterprise Security Profile Pt2
6.1.4	Enterprise Security Profile Pt2	6.1 Policy Decision Point (PDP) & Policy Orchestration	Advanced ZT	12.5	The minimum number of Enterprise Security Profile(s) exist granting access to the widest range of DAAS across Pillars within the DoD Organizations. Mission/task organization profiles are integrated with the Enterprise Security Profile(s) and exceptions are managed in a risk based methodical approach.	Enterprise Profile(s) have been reduced and simplified to support widest array of access to DAAS; Where appropriate Mission/Task Critical profile(s) have been integrated and supported Organization profiles are considered the exception	Enterprise Security Profile Pt1	Real-Time Access Decisions AI-enabled Dynamic Access Control
6.2.1	Task Automation Analysis	6.2 Critical Process Automation	Target Level ZT	6.3	DoD Organizations 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 possible retirement.	Automatable tasks are identified; Tasks are enumerated		
6.2.2	Enterprise Integration & Workflow Provisioning Pt1	6.2 Critical Process Automation	Target Level ZT	23.4	The DoD enterprise establishes baseline integrations within the Security Orchestration, Automation and Response solution (SOAR) required to enable target level ZTA functionality. DoD organizations identify integration points and prioritize key ones per the DoD enterprise baseline. Critical integrations occur meeting key services enabling recovery and protection capabilities.	Implement full enterprise integration; Identify key integrations; Identify recovery and protection requirements		Enterprise Integration & Workflow Provisioning Pt2
6.2.3	Enterprise Integration & Workflow Provisioning Pt2	6.2 Critical Process Automation	Advanced ZT	12.7	DoD Organizations integrate remaining services to meet baseline requirements and advanced ZTA functionality requirements as appropriate per environment. Service provisioning is integrated and automated into workflows where required meeting ZTA target functionalities.	Services identified; Service provisioning is implemented	Enterprise Integration & Workflow Provisioning Pt1	Automated Workflow
6.3.1	Implement Data Tagging & Classification ML Tools	6.3 Machine Learning	Target Level ZT	16.0	DoD Organizations utilize existing Data Tagging and Classification standards and requirements to procure Machine Learning solution(s) as needed. Machine Learning solution(s) is implemented in organizations and existing tagged and classified data repositories are used to establish baselines. Machine learning solution(s) applies data tags in a supervised approach to continually improve analysis.	Implemented data tagging and classification tools are integrated with ML tools	Define Data Tagging Standards	Automated Data Tagging & Support Pt1
6.4.1	Implement AI automation tools	6.4 Artificial Intelligence	Advanced ZT	25.7	DoD Organizations identify areas of improvement based on existing machine learning techniques for Artificial Intelligence. AI solutions are identified, procured, and implemented using the identified areas as requirements.	Develop AI Tool Requirements; Procure and Implement AI Tools		Automated Workflow

ID#	Activity Name	Associated Capability	Phase	Duration (months)	Descriptions	Outcomes	Predecessor(s)	Successor(s)
6.4.2	AI Driven by Analytics decides A&O modifications	6.4 Artificial Intelligence	Advanced ZT	42.0	DoD Organizations utilizing existing machine learning 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.	AI is able to make changes to automated workflow activities		
6.5.1	Response Automation Analysis	6.5 Security Orchestration, Automation & Response (SOAR)	Target Level ZT	9.0	DoD Organizations identify and enumerate all response activities that executed both manually and in an automated fashion. Response activities are organized into automated and manual categories. Manual activities are analyzed for possible retirement.	Automatable response activities are identified; Response activities are enumerated		
6.5.2	Implement SOAR Tools	6.5 Security Orchestration, Automation & Response (SOAR)	Target Level ZT	14.9	DoD enterprise working with Organizations develops a standard set of requirements for security orchestration, automation, and response (SOAR) tooling to enable target level ZTA functions. DoD Organizations use approved requirements to procure and implement SOAR solution. Basic infrastructure integrations for future SOAR functionality is completed.	Develop requirements for SOAR tool; Procure SOAR tools	Standardized API Calls & Schemas Pt1; Workflow Enrichment Pt1	
6.5.3	Implement Playbooks	6.5 Security Orchestration, Automation & Response (SOAR)	Advanced ZT	14.0	DoD organizations 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.	When possible automated playbooks based on automated workflows capability; Manual Playbooks are developed and implemented		
6.6.1	Tool Compliance Analysis	6.6 API Standardization	Target Level ZT	7.3	Automation and Orchestration tooling and solutions are analyzed for compliance and capabilities based on the DoD Enterprise programmatic interface standard and requirements. Any additional tooling or solutions are identified to support the programmatic interface standards and requirements.	API status is determined compliance or non-compliance to API standards; Tools to be used are Identified		
6.6.2	Standardized API Calls & Schemas Pt1	6.6 API Standardization	Target Level ZT	13.6	The DoD enterprise works with organizations to establish a programmatic interface (e.g., API) standard and requirements as needed to enable target ZTA functionalities. DoD Organizations update programmatic interfaces to the new standard and mandate newly acquired/developed tools to meet the new standard. Tools unable to meet the standard are allowed by exception using a risk based methodical approach.	Initial calls and schemas are implemented; Non-compliant tools are replaced		Implement SDN Programable Infrastructure; Implement SOAR Tools; Standardized API Calls & Schemas Pt2
6.6.3	Standardized API Calls & Schemas Pt2	6.6 API Standardization	Target Level ZT	14.2	DoD Organizations complete the migration to the new programmatic interface standard. Tools marked for decommission in the previous activity are retired and functions are migrated to modernized tools. Approved schemas are adopted based on the DoD Enterprise standard/requirements.	All calls and schemas are implemented	Standardized API Calls & Schemas Pt1	
6.7.1	Workflow Enrichment Pt1	6.7 Security Operations Center (SOC) & Incident Response (IR)	Target Level ZT	7.3	DoD Enterprise works with organizations to establish a cybersecurity incident response standard using industry best practices such as NIST. DoD Organizations utilize the enterprise standard to determine incident response workflows. External sources of enrichment are identified for future integration.	Threat events are identified; Workflows for threat events are developed		Implement SOAR Tools; Workflow Enrichment Pt2
6.7.2	Workflow Enrichment Pt2	6.7 Security Operations Center (SOC) & Incident Response (IR)	Target Level ZT	9.1	DoD organizations identify and establish extended workflows for additional incident response types. Initial enrichment data sources are used for existing workflows. Additional enrichment sources are identified for future integrations.	Workflows for Advanced threat events are developed; Advanced Threat events are identified	Workflow Enrichment Pt1	Workflow Enrichment Pt3
6.7.3	Workflow Enrichment Pt3	6.7 Security Operations Center (SOC) & Incident Response (IR)	Advanced ZT	12.4	DoD organizations use final enrichment data sources on basic and extended threat response workflows.	Enrichment data has been identified; Enrichment data is integrated into workflows	Workflow Enrichment Pt2	Automated Workflow
6.7.4	Automated Workflow	6.7 Security Operations Center (SOC) & Incident Response (IR)	Advanced ZT	14.4	DoD organizations 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.	Workflow processes are fully automated; Manual Processes have been identified; Remaining Processes are marked as exceptions and documented	Workflow Enrichment Pt3; Implement AI automation tools; Enterprise Integration & Workflow Provisioning Pt2	Continuous Authorization to Operate (cATO) Pt2

DoD Zero Trust Activities

ID#	Activity Name	Associated Capability	Phase	Duration (months)	Descriptions	Outcomes	Predecessor(s)	Successor(s)
7.1.1	Scale Considerations	7.1 Log All Traffic (Network, Data, Apps, Users)	Target Level ZT	11.6	DoD Organizations conduct analysis to determine current and future needs of scaling. Scaling is analyzed following common industry best practice methods and ZT Pillars. The team works with existing Business Continuity Planning (BCP) and Disaster Recovery Planning (DPR) groups to determine distributed environment needs in emergencies and as organizations grow.	Sufficient infrastructure in place; Distributed environment established; Sufficient bandwidth for network traffic		
7.1.2	Log Parsing	7.1 Log All Traffic (Network, Data, Apps, Users)	Target Level ZT	6.3	DoD Organizations 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 Organizations and implemented in future procurement requirements. Existing solutions and technologies are migrated to the format on a continual basis.	Standardized log formats; Rules developed for each log format		Implement Analytics Tools; Asset ID & Alert Correlation
7.1.3	Log Analysis	7.1 Log All Traffic (Network, Data, Apps, Users)	Target Level ZT	10.3	Common user and device activities are identified and prioritized based on risk. Activities deemed the most simplistic and risky have analytics created using different data sources such as logs. Trends and patterns are developed based on the analytics collected to look at activities over longer periods of time.	Develop analytics per activity; Identify activities to analyze		Establish User Baseline Behavior; User/Device Baselines; Baseline & Profiling Pt1
7.2.1	Threat Alerting Pt1	7.2 Security Information and Event Management (SIEM)	Target Level ZT	7.5	DoD Organizations utilize existing Security Information and Event Management (SIEM) solution to develop basic rules and alerts for common threat events (malware, phishing, etc.) Alerts and/or rule firings are fed into the parallel "Asset ID & Alert Correlation" activity to being automation of responses.	Rules developed for threat correlation		Threat Alerting Pt2; Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt1
7.2.2	Threat Alerting Pt2	7.2 Security Information and Event Management (SIEM)	Target Level ZT	16.5	DoD Organizations 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.	Develop analytics to detect deviations	Threat Alerting Pt1; Cyber Threat Intelligence Program Pt1	Threat Alerting Pt3
7.2.3	Threat Alerting Pt3	7.2 Security Information and Event Management (SIEM)	Advanced ZT	12.9	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.	Identify Triggering Anomalous Events; Implement Triggering Policy	Threat Alerting Pt2; Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt2	Continuous Authorization to Operate (cATO) Pt2
7.2.4	Asset ID & Alert Correlation	7.2 Security Information and Event Management (SIEM)	Target Level ZT	10.2	DoD Organizations develop basic correlation rules using asset and alert data. Response to common threat events (e.g., malware, phishing, etc.) are automated within the Security Information and Event Management (SIEM) solution.	Rules developed for asset ID based responses	Log Parsing	
7.2.5	User/Device Baselines	7.2 Security Information and Event Management (SIEM)	Target Level ZT	13.0	DoD Organizations develop user and device baseline approaches based on DoD Enterprise standards for the appropriate pillar. Attributes utilized in baselining are pulled from the enterprise wide standards developed in cross pillar activities.	Identify user and device baselines	Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling; Log Analysis	User Activity Monitoring Pt1; Entity Activity Monitoring Pt1
7.3.1	Implement Analytics Tools	7.3 Common Security and Risk Analytics	Target Level ZT	12.1	DoD Organizations procure and implement basic Cyber-focused analytics tools. Analytics development is prioritized based on risk and complexity looking for easy impactful analytics first. Continued analytics development focuses on Pillar requirements to better meet reporting needs.	Develop requirements for analytic environment; Procure and implement analytic tools	Log Parsing	
7.3.2	Establish User Baseline Behavior	7.3 Common Security and Risk Analytics	Target Level ZT	13.8	Utilizing the analytics developed for users and devices in a parallel activity, baselines are established in a technical solution. These baselines are applied to an identified set of users based on risk initially and then expanded to the larger DoD Organization user base. The technical solution used is integrated with machine learning functionality to begin automation.	Identify users for baseline; Establish ML-based baselines	Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling; Log Analysis	
7.4.1	Baseline & Profiling Pt1	7.4 User and Entity Behavior Analytics	Target Level ZT	12.3	Utilizing the analytics developed for users and devices in a parallel activity, common profiles are created for typical user and device types. Analytics taken from baselining are updated to look at larger containers, profiles.	Develop analytics to detect changing threat conditions; Identify user and device threat profiles	Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling; Log Analysis	Baseline & Profiling Pt2; UEBA Baseline Support Pt 1

DoD Zero Trust Activities

ID#	Activity Name	Associated Capability	Phase	Duration (months)	Descriptions	Outcomes	Predecessor(s)	Successor(s)
7.4.2	Baseline & Profiling Pt2	7.4 User and Entity Behavior Analytics	Advanced ZT	22.7	DoD Organizations 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.	Add threat profiles for IoT and OT devices; Develop and extend analytics; Extend threat profiles to individual users and devices	Baseline & Profiling Pt1	
7.4.3	UEBA Baseline Support Pt 1	7.4 User and Entity Behavior Analytics	Advanced ZT	6.3	User & Entity Behavior Analytics (UEBA) within DoD Organizations expands monitoring to advanced analytics such as Machine Learning (ML). These results are in turn reviewed and fed back into the ML algorithms to improve detection and response.	Implement ML-based Analytics to detect anomalies	Baseline & Profiling Pt1	AI-enabled Network Access; UEBA Baseline Support Pt2
7.4.4	UEBA Baseline Support Pt 2	7.4 User and Entity Behavior Analytics	Advanced ZT	6.3	User & Entity Behavior Analytics (UEBA) within DoD Organizations completes it expansion by using traditional and machine learning (ML) based results to be fed into Artificial Intelligence (AI) algorithms. Initially AI based detections are supervised but ultimately using advanced techniques such as neural networks, UEBA operators are not part of the learning process	Implement ML-based Analytics to detect anomalies	UEBA Baseline Support Pt1	
7.5.1	Cyber Threat Intelligence Program Pt1	7.5 Threat Intelligence Integration	Target Level ZT	9.9	The DoD Enterprise works with the Organizations to develop and Cyber Threat Intelligence (CTI) program policy, standard and process. Organizations utilize this documentation to develop organizational CTI teams with key mission/task stakeholders. CTI Teams integrate common feeds of data with the Security Information and Event Management (SIEM) for improved alerting and response. Integrations with Device and Network enforcement points (e.g., Firewalls, Endpoint Security Suites, etc.) are created to conduct basic monitoring of CTI driven data.	Cyber Threat Intelligence team is in place with critical stakeholders; Public and Baseline CTI feeds are being utilized by SIEM for alerting; Basic integration points exist with Device and Network enforcement points (e.g., NGAV, NGFW, NG-IPS)		Cyber Threat Intelligence Program Pt2; Threat Alerting Pt 2
7.5.2	Cyber Threat Intelligence Program Pt2	7.5 Threat Intelligence Integration	Target Level ZT	19.5	DoD Organizations expand their Cyber Threat Intelligence (CTI) teams to include new stakeholders as appropriate. Authenticated, private and controlled CTI data feeds are integrated into Security Information and Event Management (SIEM) and enforcement points from the Device, User, Network and Data pillars.	Cyber Threat Intelligence team is in place with extended stakeholders as appropriate; Controlled and Private feed are being utilized by SIEM and other appropriate Analytics tools for alerting and monitoring; Integration is in place for extended enforcement points within the Device, User, Network and Data pillars (UEBA, UAM)	Cyber Threat Intelligence Program Pt1	
7.6.1	AI-enabled Network Access	7.6 Automated Dynamic Policies	Advanced ZT	27.8	DoD Organizations utilize the SDN Infrastructure and Enterprise Security Profiles to enable Artificial Intelligence (AI)/Machine Learning (ML) driven network access. Analytics from previous activities is used to teach the AI/ML algorithms improving decision making.	Network Access is AI driven based on environment analytics	UEBA Baseline Support Pt1; Periodic Authentication; Rule Based Dynamic Access Pt1 The following activities are to be completed in parallel: Comprehensive Data Activity Monitoring User Activity Monitoring Pt2 Entity Activity Monitoring Pt2	Real-Time Access Decisions; AI-enabled Dynamic Access Control
7.6.2	AI-enabled Dynamic Access Control	7.6 Automated Dynamic Policies	Advanced ZT	24.4	DoD Organizations utilize previous rule based dynamic access to teach Artificial Intelligence (AI)/Machine Learning (ML) algorithms to make access decision to various resources. The “AI-enabled Network Access” activity algorithms are updated to enable broader decision making to all DAAS.	JIT/JEA are integrated with AI; Access is AI driven based on environment analytics	Continuous Authentication Pt2; AI-enabled Network Access	