1. **Responsibility** - The current official activities publication (6 Jan, 2023) was not clear on what activities or parts of activities components were responsible for accomplishing versus DoD top-level enterprise responsibility. This column aims to provide to clarify where the responsibility lies. When it is both an enterprise and component activity responsibility, the delineation of responsibility is in the "Activity Outcomes". The following is how the Zero Trust Portfolio Management Office defines "Enterprise" and "Component".

> **Enterprise** - Refers to management at the head of the DoD Enterprise who have a responsibility to develop policies, standards, instructions, directives, etc. and enterprise technologies (e.g. ICAM) that set the boundaries and limits for all DoD components.
>
> **Component** - Refers to OSD, the Chairman, Joint Chiefs of Staff and the Joint Staff, the DoD Inspector General, the Military Departments including the Coast Guard when assigned to the Department of the Navy, the Defense Agencies, DoD Field Activities, the Combatant Commands, Washington Headquarters Services, the Uniformed Services University of the Health Sciences, and all non-appropriated fund instrumentalities as defined per DAU.

2. **Activity Endstate** - The initial activity publication and outcomes resulted in a number questions about what each activity was ultimately mean to accomplish. These statements were meant to provide this clarification.

3. **Updates -** Only the target level zero trust activities are updated in this revision. The next revision will update the advanced level zero trust activities.

Notes

1. **National Security Systems (NSS)** - 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. **Courses of Action (COAs)** - The DoD Zero Trust Execution Roadmap briefing is no longer focused on COA 1 only. However, in the Activities tab, Columns labeled "Durations", "Predecessor", and "Successor" still maintain a COA 1 alignment to provide components with a potential schedule and dependencies to support planning and prioritization. ***These durations are notional; the mandated deadline to achieve Target Level Zero Trust remains the end of FY2027.***

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

DoD Zero Trust Capabilities

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Associated Activities
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
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

DoD Zero Trust Capabilities

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Associated Activities
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
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

DoD Zero Trust Capabilities

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Associated Activities
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

DoD Zero Trust Capabilities

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Associated Activities
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
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

DoD Zero Trust Capabilities

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Associated Activities
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
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

DoD Zero Trust Capabilities

ID #	Capability	Pillar	Capability Description	Capability Outcome	Impact to ZT	Associated Activities
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

ID#	Activity Name	Pillar	Responsibility	Activity Type	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
1.1.1	Inventory User	User	Component	Target Level ZT	25.9	DoD Components utilize Enterprise authoritative source of (PE/NPE) identity (PE - AMID, NIS, AFID) and/or establish or augment with local authoritative source. Identity management can be done manually if needed, preparing for automated approach in later stages. Identity source is connected to identity life cycle management processes (i.e. joiner/mover/leaver/returner). IT privileged users are clearly identified.	1. Identified managed non-privileged users. 2. Identified managed privileged users. 3. Identified applications using their own user account management for non-administrative and administrative accounts. 4. Identify the authoritative source of identities.	Accurately determine and keep track of users who have both the authorization and authentication to access critical systems or resources. This involves regularly reviewing, communicating, and carefully examining the sources of information that provide the true and up-to-date user data.		Rule Based Dynamic Access Pt1
1.2.1	Implement App Based Permissions per Enterprise	User	Enterprise and Component	Target Level ZT	17.7	DoD Components utilize Enterprise authoritative source of (PE/NPE) identity (PE - AMID, NIS, AFID) and/or establish or augment with local authoritative source. Identity management can be done manually if needed, preparing for automated approach in later stages. Identity source is connected to identity life cycle management processes (i.e. joiner/mover/leaver/returner). IT privileged users are clearly identified.	1. Enterprise roles/attributes needed for user authorization to application functions and/or data have been-vetted and approved through the ICAM governance processes. 2. Approved Component ICAM implementations will maintain and make available authoritative information about their personnel (i.e. attributes and entitlements), while maximizing the usage of self-service attributes and entitlements. 3. Components identify attributes associated with PAM activities within their environment. 4. Component ICAM implementation obtain authoritative information about personnel (i.e. attributes, and entitlements) from a central attribute source once. available, or from other Components using standard profiles.	Authoritative attributes requiired to implement conditional user access into applications are available to support privileged access management.		
1.2.2	Rule Based Dynamic Access Pt1	User	Component	Target Level ZT	22.1	DoD Components utilize the rules from the "Periodic Authentication" activity to build rules enabling and disabling privileges dynamically. IT Privileged user accounts utilize the PAM solution to move to dynamic privileged access using Just-in-Time (JIT) access and Just-Enough-Administration (JEA) methods.	1. Access to an applications'/services' functions and/or data are limited to users with appropriate Attribute-Based Access Control (users, devices, environment etc.), allowing for granular and flexible control. 2. All possible applications use JIT/JEA permissions for administrative users.	Periodic challenges occur where access is affected if challenge is failed within accepted response parameters. Access is always predicated on authentication and authorization with activity happening (decisions made) in real-time.	Single Authentication; Inventory User	Rule Based Dynamic Access Pt2; AI-enabled Network Access
1.2.3	Rule Based Dynamic Access Pt2	User		Advanced Level ZT	15.5	DoD Components expand the development of rules for dynamic access decision making accounting for risk. Solutions used for dynamic access are integrated with cross pillar Machine Learning (ML) and Artificial Intelligence (AI) functionality enabling automated rule management.	1. Components and services are fully utilizing rules to enable dynamic access to applications and services. 2. 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	User		Advanced Level ZT	11.6	DoD Components federate remaining user and group attributes as appropriate to the Enterprise Identity, Credential and Access Management (ICAM) solution. The updated attribute set is used to create universal roles for Organizations to use. Core functions of the Identity Provider (IdP) and ICAM solutions are migrated to cloud services and/or environments enabling improved resilience and performance.	1. Component attribute and role data repository federated with Enterprise ICAM. 2.Cloud-based Enterprise IdP can be used by cloud and on-premises applications. 3. 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	User		Advanced Level ZT	11.2	DoD Components move all possible functions of the Identity Provider (IdP) and Identity, Credential and Access Management (ICAM) solutions to cloud environments. Enclave/Denied, Disrupted, Intermittent, and Limited (DDIL) environments utilize local capabilities to support disconnected functions but ultimately are managed by the centralized ICAM. Updated roles are now mandated for usage and exceptions are reviewed following a risk-based approach.	1. Components utilize cloud IdP functionality Where possible on-premise IdP is decommissioned. 2. Permissions and roles are mandated for usage when evaluating attributes.		Enterprise Gov't roles and Permissions Pt1	
1.3.1	Organizational MFA/IDP	User	Component	Target Level ZT	10.6	DoD Components or Identity Provider (IdP) solution using approved credential or approved alternative Multi-Factor Authentication (MFA). The IdP and MFA solution may be combined in a single application or separated as needed assuming automated integration is supported by both solutions. Both IdP and MFA support integration with the Enterprise PKI capability as well as enabling key pairs to be signed by the trusted root certificate authorities. Authentication for mission/task-critical applications and services authentication is MFA-Enabled and leverages the related authentication mechanisms to manage users and groups.	1. Component is using IdP with MFA for critical applications/services. 2. Components have implemented an Identity Provider (IdP) that enables DoD PKI Multi-Factor Authentication (e.g. CAC, DPIV, DoD Issued PIV-I, FIPS 201 Compliant softcerts). 3. DoD Enterprise is the approved organizational PKI for critical services (ECA, FPKI, Category I/II/III PKI, etc.). 4. Utilize approved Alternative Hardware Tokens as needed - USB Security Key and/or OTP device (e.g. Yubikey FIPS for smartcard, FIDO2, FIDO U2F, OTP, RSA SecurID for OTP, etc.). 5. For access to low-risk resources (e.g., PII, publicly released information), utilize alternative two-step, two-factor authentication using software authenticators (i.e., Mobile Connect, Yubico, Okta Verify, etc.).	Critical applications are identified and use MFA in alignment with a federated IdP solution.		

ID#	Activity Name	Pillar	Responsibility	Activity Type	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
1.3.2	Alternative Flexible MFA Pt1	User		Advanced Level ZT	17.4	DoD Components Identity Provider (IdP) supports alternative methods of Multi-Factor Authentication (MFA) complying with Cyber Security requirements (e.g., FIPS 140-2, FIPS 197, etc.). Alternative tokens can be used for application-based authentication. MFA options support biometric capability and can be managed using a self-service approach. Where possible MFA provider(s) are moved to cloud services instead of being hosted on-premise.	1. IdP provides user self-service for alternative MFA options for approved applications. 2. IdP provides alternative token MFA for approved applications per policy.		Organizational MFA/IDP	Alternative Flexible MFA Pt2
1.3.3	Alternative Flexible MFA Pt2	User		Advanced Level ZT	14.6	Alternative Multi-Factor Authentication (MFA) methods utilize user activity patterns from cross pillar activities such as "User Activity Monitoring (UAM) and User & Entity Behavior Analytics (UEBA)" to assist with access decision making (e.g., not grant access when pattern deviation occurs).	1. User activity patterns implemented.		Alternative Flexible MFA Pt1	
1.4.1	Implement System and Migrate Privileged Users Pt1	User	Component	Target Level ZT	12.4	DoD Components procure and implement a Privileged Access Management (PAM) solution to support all critical privileged use cases. Application/Service integration points are identified to determine status of support for the PAM solution. Applications/Services that easily integrate with the PAM solution are transitioned to using the solution versus static and direct privileged permissions.	1. Privilege Access Management (PAM) tooling is implemented. 2. Applications and devices that support and do not support PAM tools are identified. 3. Applications that support PAM, now use PAM for controlling emergency/built-in accounts.	Components implement a PAM tool with a clear transition plan that identifies the applications and decides what applications require a PAM tool.		Implement System and Migrate Privileged Users Pt2
1.4.2	Implement System and Migrate Privileged Users Pt2	User	Component	Target Level ZT	14.4	DoD Components utilize the inventory of supported and unsupported Applications/Services for integration with the Privileged Access Management (PAM) solution to extend integrations. PAM is integrated with the more challenging Applications/Services to maximize PAM solution coverage. Exceptions are managed in a risk-based methodical approach with the goal of migration off and/or decommissioning Applications/Services that do not support the PAM solution.	1. Privileged activities are migrated to PAM and access is fully managed.	Ensure secure and controlled access to privileged accounts and resources through fully implemented PAM solution, mitigating the risk of unauthorized access and potential cyber threats.	Implement System and Migrate Privileged Users Pt1	Real time Approvals & JIT/JEA Analytics Pt1
1.4.3	Real time Approvals & JIT/JEA Analytics Pt1	User		Advanced Level 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.	1. Accounts, applications, and data of concern (of greatest risk to DoD mission) are identified. 2. Using PAM tools, access to applications/services follows JIT/JEA methodology 3. Privileged access requests are automated as appropriate.		Implement System and Migrate Privileged Users Pt2	Real time Approvals & JIT/JEA Analytics Pt2
1.4.4	Real time Approvals & JIT/JEA Analytics Pt2	User		Advanced Level ZT	8.9	DoD Components integrate User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions with the Privileged Access Management (PAM) solution providing user pattern analytics for decision making.	1. 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	User	Component	Target Level ZT	14.8	DoD Components establish a process for life cycle management of users both privileged and non-privileged. Utilizing an approved Identity Provider (IdP) the process is implemented and followed by the maximum number of users. Users falling outside of the standard process are approved through risk-based exceptions to be evaluated regularly for decommission.	1. Standardized account life cycle process.	Establishes a comprehensive and efficient process that ensures the accurate and secure management of user identities throughout their entire life cycle within the Components environment.		Enterprise Identity Life-Cycle Management Pt1
1.5.2	Enterprise Identity Life-Cycle Management Pt 1	User	Enterprise and Component	Target Level ZT	11.7	Specified policies and supporting process are followed by DoD Components. DoD Components implement the Enterprise Identity Life-Cycle Management process for the maximum number of identities, attributes, groups, credentials, and permissions. Exceptions to the policy are managed in a risk-based methodical approach.	1. Automated identity life cycle processes. 2. Integrated with Enterprise ICAM process and tools.	Implemention of consistent and well-defined processes and controls for managing the maximum number of identities in the life cycle.	Organizational Identity Life-Cycle Management	Enterprise Identity LifeCycle Management Pt2
1.5.3	Enterprise Identity LifeCycle Management Pt2	User		Advanced Level ZT	12.8	DoD Components further integrate the critical automation functions of the Identity Provider (IdP) and Identity, Credential and Access Management (ICAM) solutions following the Enterprise Identity Life-Cycle Management (ILM) process to enable Enterprise automation and analytics. ILM primary processes are integrated into the cloud-based Enterprise ICAM solution.	1. Integration with Critical IDM/IdP functions. 2. Primary ILM functions are cloud based.		Enterprise Identity Life-Cycle Management Pt1	Enterprise Identity LifeCycle Management Pt3

ID#	Activity Name	Pillar	Responsibility	Activity Type	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
1.5.4	Enterprise Identity LifeCycle Management Pt3	User		Advanced Level ZT	9.2	DoD Components integrate remaining Identity Lifecycle Management (ILM) processes with the Enterprise Identity, Credential and Access Management (ICAM) solution. Enclave/DDIL environments, while still authorized to operate, integrate with the Enterprise ICAM using local connectors to the cloud environment.	1. All ILM functions moved to cloud as appropriate. 2. Integration with all IDM/IdP functions.		Enterprise Identity LifeCycle Management Pt2	
1.6.1	Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling	User	Component	Target Level ZT	15.9	DoD Components procure and implement User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions. Initial integration point with Enterprise IdP is completed, enabling future usage in decision making.	1. UEBA and UAM functionality is correlated with the Master User Record and integrated with Enterprise IdP.	Establish a comprehensive and continuously adaptive security solution that leverages behavior analytics, detects anomalies, and protects against unauthorized access.		Establish User Baseline Behavior; User/Device Baselines Alternative Flexible MFA PT2
1.6.2	User Activity Monitoring Pt1	User		Advanced Level ZT	13.5	DoD Components integrate User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions with Identity Providers (IdP) for extended visibility as needed. Analytics and data generated by UEBA and UAM for critical applications/services are integrated with Just-in-Time (JIT) and Just-Enough-Access (JEA) solutions for improving decision.	1. UEBA is integrated with IdPs as appropriate. 2. UEBA is integrated with JIT/JEA for critical services.		User/Device Baselines	User Activity Monitoring Pt2
1.6.3	User Activity Monitoring Pt2	User		Advanced Level ZT	11.2	DoD Components continue the analytics usage from User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions by using generated data for all monitored applications and services when decision making occurs in the Just-in-Time (JIT) and Just-Enough-Access (JEA) solution.	1. UEBA and UAM is integrated with JIT/JEA for all services.		User Activity Monitoring Pt1	Real-Time Access Decisions; Alenabled Dynamic Access Control; Enrich Attributes for Resource Authorization Pt1; AI-enabled Network Access
1.7.1	Deny User by Default Policy	User	Component	Target Level ZT	22.7	DoD Components audit user and group usage for permissions and revoke permissions when appropriate. This activity includes the revocation and/or decommission of excess permissions and access for application/service-based identities and groups. Where possible, static privileged users are decommissioned or permission are reduced, preparing for future rule/dynamic based access. The implemented audit and governance functions are automated where possible.	1. Applications updated to deny by default to functions/data requiring specific roles/attributes for access. 2. Reduced default permission levels are implemented. 3. Applications/services privileged users have been reviewed and audited, and unnecessary access has been removed. 4. Applications' identify functions and data requiring specific roles/attributes for access. 5. Audit functions and governance processes are implemented and automated when possible to update user authentication and authorization.	Users must be authorized and authenticated to access data, applications, assets, and services. Audit and access validation occurs consistently.		
1.8.1	Single Authentication	User	Component	Target Level ZT	19.2	DoD Components authenticate users and NPEs at least once per session (e.g., logon) using CAC and other DoD approved methods. Users being authenticated are managed by the parallel activity "Organizational MFA/IdP" with the Component Identity Provider (IdP). Components do not use application/service-based identities and groups.	1. Authentication implemented at least once per session.	Component applications apply single authentication to the specified standard.		Rule Based Dynamic Access Pt1 Resource Authorization Pt1; SDC Resource Authorization Pt2
1.8.2	Periodic Authentication	User	Component	Target Level ZT	25.4	DoD Components enable periodic authentication for applications and services. Traditionally, these are based on duration and/or duration timeout, however, other period-based analytics can be used to enforce re-authentication of user sessions.	1. Authentication implemented multiple times per session based on security attributes and criticality of the data, user, application, system, and source user location.	Authentication occurs per the requirement and standard.	Single Authentication	Continuous Authentication Pt1; AI-enabled Network Access
1.8.3	Continuous Authentication Pt 1	User		Advanced Level ZT	16.8	DoD Components applications/services utilize multiple session authentications based on security attributes and access requested. Privilege changes and associational transaction requests require additional levels of authentication such as Multi-Factor Authentication (MFA) pushes to users.	1. Transaction authentication implemented per session based on security attributes.		Periodic Authentication	Continuous Authentication Pt2
1.8.4	Continuous Authentication Pt 2	User		Advanced Level ZT	16.8	DoD Components continue usage of transaction-based authentication to include integration such as user patterns.	1. Transaction authentication implemented per session based on security attributes.		Continuous Authentication Pt1	Real-Time Access Decisions; Alenabled Dynamic Access Control
1.9.1	Enterprise PKI/IDP Pt1	User	Enterprise and Component	Target Level ZT	12.4	The DoD Enterprise works with Components to implement Enterprise Public Key Infrastructure (PKI) solutions in a centralized and/or federated fashion. The Enterprise PKI solution utilizes a single or set of Enterprise level Root Certificate Authorities (CA) that can then be trusted by components to build Intermediate CA. Components PKI Certificated Authorities are integrated with the Enterprise PKI. An Enterprise Identity Provider (IdP) platform is implemented. The IdP solution may either be a single solution or federated set of Component IdPs with standard level of access across Components and standardized set of attributes. Components IdPs are integrated with the Enterprise IdP.	1. Enterprise PE & NPE CONOPS, taxonomy, and naming standards are developed. 2. Components Certificate Authorities (CA) are integrated with the DoD PKI Hierarchy. 3. Enterprise level requirements are implemented, including mandated user attributes for a validated and verified Enterprise Identity Provider (IdP) Platform. 4. Enterprise wide IdP platform is implemented through a single solution or integration of multiple solutions.	All PEs and NPEs are issued a validated and verified digital identity that can be tracked at the Enterprise level using the strongest authentication available.		Enterprise PKI/IDP Pt2

ID#	Activity Name	Pillar	Responsibility	Activity Type	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
1.9.2	Enterprise PKI/IDP Pt2	User		Advanced Level ZT	27.2	DoD Components enable biometric support in the Identity Provider (IdP) for mission/task-critical applications and services as appropriate. Biometric functionality is moved from Component solutions to the Enterprise. Multi-Factor Authentication (MFA) and Public Key Infrastructure (PKI) is decommissioned and migrated to the Enterprise as appropriate.	1. Critical services integrated with biometrics. 2. Decommission organizational MFA/PKI as appropriate in lieu of Enterprise MFA/PKI. 3. Enterprise biometric functions implemented.		Enterprise PKI/IDP Pt1	Enterprise PKI/IDP Pt3
1.9.3	Enterprise PKI/IDP Pt3	User		Advanced Level ZT	30.0	DoD Components integrate the remaining applications/services with Biometrics functionalities. Alternative Multi-Factor Authentication (MFA) tokens can be used.	1. All Components services integrate with biometrics.		Enterprise PKI/IDP Pt2	
2.1.1	Device Health Tool Gap Analysis	Device	Component	Target Level ZT	9.8	DoD Components develop an inventory of devices within the environment, and device attributes are tracked.	1. Inventory of authorized and approved devices is created per Component with owners. 2. Determine and implement tools to gauge device health.	A comprehensive inventory of authorized and approved devices with designated owners, and effective tools for monitoring and assessing device health are implemented.		
2.1.2	NPE/PKI, Device under Management	Device	Component	Target Level ZT	22.8	DoD Components utilize the DoD Enterprise PKI solution/service to deploy x509 certificates to all supported and managed devices. Other Non-Person Entities (NPEs) (e.g., web servers, network devices, routers, applications, etc.) that support x509 certificates are assigned them in the PKI and/or IdP systems.	1. Non-person entities are managed via Component PKI and IdP.	Components use established PKI and IdP solutions to manage all NPEs.	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	Device	Enterprise and Component	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.	1. Component NPEs are integrated with Enterprise IdP. 2. Where applicable, ensure tracking in the UEM solution.	All NPEs are assigned static attributes in an identity provider, provided an exception based on risk analysis, or marked for retirement, as part of the Enterprise Life Cycle Management plan.		Enterprise IDP Pt2
2.1.4	Enterprise IDP Pt2	Device		Advanced Level ZT	8.8	The DoD Enterprise Identity Provider (IdP), either using a centralized technology or federated organizational technologies, adds additional attributes for Non-Person Entities (NPEs) (e.g., location, usage patterns, etc.) to device profiles.	1. Conditional device attributes are part of the IdP profile.		Enterprise IDP Pt1	
2.2.1	Implement C2C/Compliance Based Network Authorization Pt1	Device	Enterprise and Component	Target Level ZT	9.4	The DoD Enterprise refines policy, standards, and requirements for Comply to Connect (C2C). Components implement and enforce-compliance-based network authorization to meet ZT Target Level functionalities.	1. C2C is enforced at the Component level for all environments. 2. All mandated device checks are implemented using C2C at the Component level.	A policy exists or is developed that dictates the need for all devices to be authorized, authenticated, and C2C compliant before connecting to the network.	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	Device		Advanced Level ZT	18.2	DoD Components expand the deployment and usage of Comply to Connect (C2C) to all supported environments required to meet ZT advanced functionalities. C2C teams integrate their solution(s) with the Enterprise IdP and Authorization Gateways to better manage access and authorizations to resources.	1. C2C is enforced in all supported environments. 2. Advanced device checks are completed and integrated with dynamic access (Enterprise IdP / Zero Trust Network Access (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	Device		Advanced Level ZT	16.4	Using the developed User and Device baselines, DoD Components utilize the implemented User and Entity Behavioral Activity (UEBA) solution to integrate baselines. UEBA device attributes and baselines are available to be used for device authorization.	1. UEBA attributes are integrated for device baselining. 2. 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	Device		Advanced Level ZT	16.7	DoD Components utilize the User and Entity Behavioral Activity (UEBA) solution with network access solutions to mandate UEBA attributes (e.g., device health, logon patterns, etc.) for accessing environments and resources.	1. UEBA attributes are mandated for device access.		Entity Activity Monitoring Pt1	Real-Time Access Decisions; Alenabled Dynamic Access Control; Enrich Attributes for Resource Authorization Pt1; AI-enabled Network Access

ID#	Activity Name	Pillar	Responsibility	Activity Type	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
2.3.3	Implement Application Control & File Integrity Monitoring (FIM) Tools	Device	Component	Target Level ZT	16.2	DoD Components procure and implement File Integrity Monitoring (FIM) and Application control (e.g., execution deny/allow listing, containment, isolation) solutions. FIM ensures any data altered is authorized, and unauthorized changes are detected by FIM. Application containment is used to isolate any suspicious behavior or permissions to prevent any malicious lateral movement, expanding the capabilities and response of traditional executable containment. Both FIMS and application containment continues the development of the Device, Data, and Application & Workload pillars.	1. Application control and FIM tooling is implemented on all service applications and endpoint devices with C2C orchestration. 2. EDR tooling covers maximum amount of services applications and endpoint devices.	Components deploy FIM and application control tooling in alignment with EDR, SOAR, and UEM. C2C orchestration and regular control audits and alerts are in place.		
2.3.4	Integrate NextGen AV Tools with C2C	Device	Component	Target Level ZT	18.5	DoD Component procures and implements an Endpoint Protection Platform (EPP). EPP should have the capabilities to use advanced analytics (e.g., artificial intelligence, behavioral detection, machine learning) to mitigate exploits (e.g., zero days, signatureless, fileless), provide Network Access Control, and protect against known and unknown threats. These solutions are orchestrated with the C2C or EDR solution for baseline status checks of signatures, updates, etc.	1. Critical Endpoint Protection Platform (EPP) data is being sent to C2C and EDR for checks. 2. EPP tooling is implemented on all critical services applications and endpoint devices.	Advanced protection on endpoint devices against modern threats, while developing Automation & Orchestration, as well as Visibility & Analytics pillar, through AI, ML and behavior analysis.		Implement C2C/Compliance Based Network Authorization Pt1
2.3.5	Fully Integrate Device Security stack with C2C as appropriate	Device		Advanced Level ZT	13.3	DoD Components continue the deployment of Application Control to all environments and in prevention mode. File Integrity Monitoring (FIM) and Application Controls analytics are integrated into Comply to Connect (C2C) for expanded access decision making. C2C analytics are evaluated for further device/endpoint security stack data points such as UEDM and are integrated as necessary.	1. Application Control and FIM deployment is expanded to all necessary services/applications. 2. Remaining data from Device Security tooling is implemented with C2C.			Implement C2C/Compliance Based Network Authorization Pt2; Managed and Full BYOD & IOT Support Pt2
2.3.6	Enterprise PKI Pt1	Device		Advanced Level ZT	22.7	The DoD Enterprise Public Key Infrastructure (PKI) is expanded to include the addition of NPE and device certificates. NPEs and devices that do not support PKI certificates are marked for retirement.	1. All devices and NPEs have certificates installed for authentication provisioned by the Enterprise PKI. 2. Devices that are unable to use certificate-based authentication are phased out and/or moved to minimal access environments.		Implement UEDM or equivalent Tools; NPE/PKI Device Under Management	Enterprise PKI Pt2
2.3.7	Enterprise PKI Pt2	Device		Advanced Level ZT	10.5	DoD Components utilize certificates provisioned by the DoD Enterprise Public Key Infrastructure (PKI) for device authentication and machine to machine communications. Unsupported devices are retired and exceptions are approved and managed using a risk based methodical approach.	1. Devices are required to authenticate with certificate-based authentication to communicate with other services and devices.		Enterprise PKI Pt1	
2.4.1	Deny Device by Default Policy	Device	Enterprise and Component	Target Level ZT	9.6	DoD Enterprise sets standards and requirements for overall policy, with Components tailoring to specific environmentse and mission requirements. DoD Components will block access from all unmanaged remote and local devices to resources. Managed compliant devices are provided risk-based, methodical access following ZT Target Level concepts.	1. Enterprise sets standards for Deny Device by Default policy. 2. Components will block unmanaged devices remotely/locally. 3. Access is enabled strictly for compliant devices remotely/locally following the "Deny Device by Default" policy" approach.	All device access is authorized, verified, and compliant and all other devices are blocked by default.	NPE/PKI Device Under Management	
2.4.2	Managed and Limited BYOD & IOT Support	Device	Enterprise and Component	Target Level ZT	39.7	DoD Components utilize Enterprise Device Management Solution to ensure that managed Bring Your Own Device (BYOD) and Internet of Things (IoT) devices are fully integrated with Enterprise IdP. Enabling user and device-based authorization is supported. Device access requires dynamic access policies and the practice of least privilege.	1. All Component access must be governed by dynamic access permissions for BYOD and IoT Devices. 2. Component BYOD and IoT device permissions are baselined and integrated with Enterprise IdP.	Components establish a foundation for risk-based access control for BYOD and IoT with dynamic permissions.		Implement C2C/Compliance Based Network Authorization Pt1; Managed and Full BYOD & IOT Support Pt1
2.4.3	Managed and Full BYOD & IOT Support Pt1	Device		Advanced Level ZT	24.7	DoD Components utilize Unified Endpoint and Device Management (UEDM) and similar solutions to enable access for managed and approved devices to Mission and Operational Critical services/applications using dynamic access policies. BYOD and Internet of Things (IoT) devices are required to meet standard baseline checks before authorization.	1. Only BYOD and IoT devices that meet configuration standards are allowed to access resources. 2. 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	Device		Advanced Level ZT	24.6	DoD Components utilize Unified Endpoint and Device Management (UEDM) and similar solutions to grant authorized managed devices access to all services and applications where possible. Unmanaged devices, upon meeting device checks and standard baselines, are granted access to services and applications following a risk-based authorization approach.	1. All possible services require dynamic access for devices.		Fully Integrate Device Security Stack w/C2C as appropriate; Managed and Full BYOD & IOT Support Pt1	

ID#	Activity Name	Pillar	Responsibility	Activity Type	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
2.5.1	Implement Asset, Vulnerability and Patch Management Tools	Device	Component	Target Level ZT	18.4	DoD Components implement solution(s) for managing asset/device configurations, vulnerabilities, and patches. Using minimum compliance standards (e.g., STIGs, C2C, UEM etc.), teams can confirm or deny managed device compliance. As part of the procurement and implementation process for solutions, APIs or other programmatic interfaces will be in scope for future levels of automation and integration.	1. Components can confirm if devices meet minimum compliance standards or not. 2. Component solutions enable integration across asset management, vulnerability, and patching systems while considering automation capabilities.	Continuously identify and address vulnerabilities, manage assets effectively, and apply necessary patches to mitigate potential threats and maintain a secure environment.		Implement C2C/Compliance Based Network Authorization Pt1; Automate Application Security & Code Remediation Pt1
2.6.1	Implement UEDM or equivalent Tools	Device	Component	Target Level ZT	18.1	DoD Components will work closely with the "Implement Asset, Vulnerability, and Patch Management Tools" activity to procure a implement and Unified Endpoint Device Management (UEDM) solution ensuring that requirements are integrated with the procurement process. Once a solution is procured the UEDM team(s) ensure that critical ZT Target Level functionalities such as minimum compliance, asset management, and API support are in place.	1. Components can confirm if devices meet minimum compliance standards or not. 2. Components have asset management system(s) for user devices (phones, desktops, laptops) that maintains IT compliance, which is reported up to DoD enterprise. 3. Components asset management systems can programmatically (i.e., API) provide device compliance status and if it meets minimum standards.	UEDM implementation enables effective patch management and configuration baselines. It also provides an ability to deny/quarantine devices remotely that are not in compliance.		Enterprise PKI Pt1
2.6.2	Enterprise Device Management Pt1	Device	Enterprise and Component	Target Level ZT	17.6	DoD Enterprise sets standards and policies for Enterprise Device Management (EDM). DoD Components migrate the manual device inventory to an automated approach using an EDM solution. Approved devices are able to be managed regardless of location. Devices part of critical services are managed by the EDM solution supporting automation.	1. Enterprise sets standards and policies for EDM. 2. Components manual inventory is integrated with an automated management solution for critical services. 3. Components enable ZT device management (from any location with or without remote access). 4. Where applicable, ensure tracking of NPEs in the UEM solution.	Implementing consistent and well-defined processes and controls for managing devices.		NPE/PKI Device Under Management; Enterprise Device Management Pt2; Resource Authorization Pt1
2.6.3	Enterprise Device Management Pt2	Device	Component	Target Level ZT	12.6	DoD Components migrate the remaining devices to Enterprise Device Management (EDM) solution. EDM solution is integrated with risk and compliance solutions as appropriate.	1. Manual inventory of devices, software, and security posture of each device is integrated with an automated management solution for all services.	All devices are managed and automation is utilized where applicable for rapid threat mitigation.	Enterprise Device Management Pt1	
2.7.1	Implement Endpoint Detection & Response (EDR) Tools and Integrate with C2C	Device	Component	Target Level ZT	16.5	DoD Components procure and implement Endpoint Detection and Response (EDR) solution(s) within environments. EDR is protecting, monitoring, and responding to malicious and anomalous activities enabling ZT Target Level functionality and is sending data to the Comply to Connect (C2C) solution for expanded device and user checks.	1. EDR tooling is implemented. 2. Critical EDR data is being sent to C2C for checks. 3. Endpoint Protection Platform (EPP) tooling covers maximum amount of services/applications.	Detect advanced threats that are undetectable by a traditional antivirus program, optimizing the response time of incidents, discarding false positives, implement blocking, and protect against multiple threats happening simultaneously across various threat vectors.	Integrate NextGen AV Tools with C2C	Implement Extended Detection & Response (XDR) Tools and Integrate w/C2C Pt 1
2.7.2	Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt1	Device	Component	Target Level ZT	19.2	DoD Components procure and implement Extended Detection & Response (XDR) solution(s). Integration points with cross pillar capabilities (network, cloud services, applications) are identified and prioritized based on risk. XDR is aligned with C2C program. XDR capabilities either supplement or replace EDR implementations. Analysis and correlation capabilities are sent from the XDR solution stack to the SIEM.	1. XDR solution is implemented,and replaces EDR where possible. 2. Integration points have been identified and prioritized per capability. 3. XDR and SIEM have integrations to gain a comprehensive view of data integration, correlation, analytics, incident response, and automation.	Expanding from an EDR to an XDR solution provides a holistic view of the threat landscape, allowing for coordinated response, automation, and orchestration when responding to threats.	Implement Endpoint Detection & Response (EDR) Tools and Integrate w/C2C; Threat Alerting Pt1	Implement Extended Detection & Response (XDR) Tools and Integrate w/C2C Pt 2
2.7.3	Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt2	Device		Advanced Level ZT	19.9	Extended Detection & Response (XDR) solution stack completes identification of integration points expanding coverage to the fullest amount possible. Exceptions are tracked and managed using a risk-based approach for continued operation. Extended analytics enabling ZT Advanced Level functionalities are integrated into the SIEM and other appropriate solutions.	1. Remaining integration points have been integrated, with exceptions for operational integrity being tracked. 2. XDR solutions, along other Analytic tools, enhance alerting and responses with SIEM, and other solutions.		Implement Extended Detection & Response (XDR) & Integrate w/C2C Pt 1	Threat Alerting Pt3
3.1.1	Application/Code Identification	Application & Workload	Component	Target Level ZT	16.7	DoD Components create an inventory of approved applications and code being used, including open-source, commercial, and in-house developed software. Each Component will track the supportability (i.e., active, legacy, etc.) hosted location (i.e., cloud, on-premises, hybrid, etc.) and record important data (i.e., name, version, team responsible, licensing and support, mapped dependencies).	1. Component has identified applications and classified as either legacy, virtualized on-premises, and cloud hosted. 2. Applications and codes are tracked by vendor, version number, commercial name, and patch level.	Develop an inventory to better support patch management and supply chain risk management increasing security by identifying unauthorized apps and identify security vulnerabilities.		
3.2.1	Build DevSecOps Software Factory Pt1	Application & Workload	Enterprise	Target Level ZT	19.3	The DoD Enterprise provide best practices for modern DevSecOps processes and CI/CD pipelines. The concepts are applied in a standardized technology stack across DoD Components able to meet future Application Security requirements, including requirements gathering, design, development, testing and deployment.	1. Developed security best practices for DevSecOps and CI/CD pipelines. 2. Vulnerability management is integrated into CI/CD pipelines.	Implementing consistent and well-defined processes and controls for DevSecOps.		Build DevSecOps Software Factory Pt2; Automate Application Security & Code Remediation Pt1

ID#	Activity Name	Pillar	Responsibility	Activity Type	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
3.2.2	Build DevSecOps Software Factory Pt2	Application & Workload	Component	Target Level ZT	10.8	DoD Components use their approved CI/CD pipelines to develop most new applications. Any exceptions will follow a standardized approval process to be allowed to develop in a legacy fashion. DevSecOps processes are also used to develop all new applications and update existing applications. Continual validation functions are integrated into the CI/CD pipelines and DevSecOps processes and integrated with existing applications.	1. Implement Component CI/CD pipeline(s) and Software Factory per the DoD CIO DevSecOps Instruction/Directive. 2. Application development adopts the use of CI/CD pipelines. 3. Continual validation process/technology is implemented and in use (see "Continual Validation" activity). 4. Application development adopts the use of the DevSecOps process and technology.	Ensure code changes and updates are secure and compliant, reducing risk of an exploit.	Build DevSecOps Software Factory Pt1	Continuous Authorization to Operate (cATO) Pt1
3.2.3	Automate Application Security & Code Remediation Pt1	Application & Workload	Enterprise and Component	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 securing API gateways (i.e., API management, WAF, continuous API testing, distributed enforcement not just perimeter) with applications utilizing API or similar calls. Code reviews are conducted in a methodical approach, and standardized protections for containers and their infrastructure are in place. Additionally, any serverless functions where the 3rd party manages the infrastructure, such as Platform as a Service, utilize adequate serverless security monitoring and response functions. Code reviews, container and serverless security functions are integrated into the CI/CD and/or DevSecOps process, as appropriate.	1. Enterprise sets standardized approach to application security, including code remediation. 2. Secure API Gateway is operational, and the majority of API calls are passing through the gateway. 3. Application Security functions (e.g., code review, container and serverless security) are implemented as part of CI/CD and DevSecOps.	Standardize and modernize security infrastructure tools and security integration into application development processes.	Vulnerability Management Program Pt2; Implement Asset, Vulnerability and Patch Management Tools; Build DevSecOps Software Factory Pt1	Automate Application Security & Code Remediation Pt2; REST API Micro-Segments
3.2.4	Automate Application Security & Code Remediation Pt2	Application & Workload		Advanced Level ZT	16.2	DoD Components modernize approaches to delivering internally developed and managed applications following best practice approaches such as a Microservices architecture. These approaches will enhance security and resilience by enabling rapid code updates within individual microservices to address vulnerabilities. Further enhance application security by integrating runtime security functions for containers where applicable, automating vulnerable library updates, and automating CI/CD approvals during the release process.	1. Secure API Gateway is operational, and majority of API calls are passing through API gateway. 2. Services are provided following a Service Oriented Architecture (SOA). 3. 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	Application & Workload	Enterprise	Target Level ZT	23.4	The DoD Enterprise uses best practices to manage approved binaries and code in a methodical approac, including supplier sourcing risk management, approved repository usage, Software Bill of Materials (SBOM), supply chain risk management, and industry-standard vulnerability management.	1. Supplier sourcing risk evaluated and identified for approved sources. 2. Repository and update channel established for use by development teams. 3. SBOMs are created for applications to identify source, supportability, and risk posture. 4. Defense Industry Base (DIB) standards and approved vulnerability databases are pulled in to be used in DevSecOps.	Safeguard the creation, storage, and delivery of code	Vulnerability Management Program Pt1	
3.3.2	Vulnerability Management Program Pt1	Application & Workload	Enterprise and Component	Target Level ZT	7.8	The DoD Enterprise collaborates with Components to establish and manage a comprehensive Vulnerability Management program. The program, at a minimum, encompasses the tracking and management of public vulnerabilities based on DoD applications and services. Each Component is responsible for establishing a vulnerability management team comprised of key stakeholders. This team convenes to discuss and manage vulnerabilities in accordance with established Enterprise policy and standards.	1. Components establish a vulnerability management governance team with appropriate stakeholder membership. 2. Enterprise provides a vulnerability management policy and standard for minimum tracking and management of public vulnerabilities based on DoD applications andservices.	Provide structure and an approach to addressing vulnerabilities in accordance with Enterprise policy.		Approved Binaries/Code; Vulnerability Management Program Pt2
3.3.3	Vulnerability Management Program Pt2	Application & Workload	Enterprise and Component	Target Level ZT	12.1	Processes are established at the DoD Enterprise level for managing the disclosure of vulnerabilities in DoD maintained and operated services, both publicly and privately accessible. DoD Components expand the vulnerability management program to track and manage closed vulnerability repositories such as DIB-VDP, CERT, and others.	1. Components utilize controlled (e.g., DIB-VDP, CERT) sources for tracking vulnerabilities. 2. Enterprise sets minimum standards for vulnerability management program accepting external/public disclosures for managed services. 3. Vulnerability remediation plans are developed and implemented at the Component level.	Enterprise-established processes for automated threat sharing from controlled sources are integrated into Component vulnerability management programs.	Vulnerability Management Program Pt1	Automate Application Security & Code Remediation Pt1
3.3.4	Continual Validation	Application & Workload	Component	Target Level ZT	11.1	DoD Components implement a continuous validation approach for application development, where security is constantly assessed throughout the development, integration, and deployment. Validation includes security principles when planning and designing, security testing (to include code reviews), incident response, and SIEM alerting/logging. These principles are integrated and continuously executed with the CI/CD pipeline. Applications developed outside of CI/CD process should still adhere to continuous validation in an ad hoc/manual manner.	1. Continual validation tools are implemented and applied to code in the CI/CD pipeline. 2. Updated applications are only deployed in a live and/or production environment with a continuous validation approach. 3. Applications developed outside of CI/CD pipeline are still validated in a ad hoc/manual manner, as established in the continuous validation approach.	Establish a continuous validation process and tooling that are seamlessly integrated with application planning and design, security testing, incident response, and SIEM alerting/logging.		

ID#	Activity Name	Pillar	Responsibility	Activity Type	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
3.4.1	Resource Authorization Pt1	Application & Workload	Enterprise and Component	Target Level ZT	18.5	The DoD Enterprise standardizes policy enforcement approaches (e.g., Software Defined Perimeter) with the Components. At a minimum, the access and authorization gateways will be integrated with identities and devices once authentication is achieved. Components deploy approved resource authorization gateways and enable them for external facing applications and services. Additional applications for migration and applications unable to be migrated are identified for exception or decommission.	1. DoD Enterprise sets standards on policy enforcement approach. At a minimum, access and authorization is integrated with identities and devices once authentication is achieved. 2. Components deploy approved resource authorization gateways and enable them for external facing applications and services. 3. DoD Enterprise-wide interoperability guidance is communicated to stakeholders.	Policy enforcement points are fully integrated with identity and device management systems, ensuring consistent and secure access control across the Enterprise.	Single Authentication; Datacenter Macro segmentation; Enterprise Device Management Pt1	Resource Authorization Pt2
3.4.2	Resource Authorization Pt2	Application & Workload	Component	Target Level ZT	20.6	Policy enforcements and decisions are used for all possible applications and services. Application unable to utilize gateways are either decommissioned or accepted using a risk-based methodical approach. Authorizations are further integrated with the CI/CD pipeline for automated decision making.	1. Policy enforcement is utilized for all applications and services. 2. Applications and services are identified that are accepted or decommissioned.	Resource authorization gateways leveraging PDP and PEP integrated with identity and access management systems are implemented for all applications. Authorization policies are embedded within DevSecOps and the CI/CD pipeline to ensure automated, continuous, and secure access control decisions.	Resource Authorization Pt1	
3.4.3	SDC Resource Authorization Pt1	Application & Workload	Enterprise and Component	Target Level ZT	31.1	The DoD Enterprise establishes best practices for code-based compute management (i.e., Software Defined Compute(SDC)). Using risk-based approaches, baselines are created using the approved set of code libraires and packages. DoD Components work with the approved code/binaries activities to ensure that applications are identified which can and cannot support the approach. Applications that can support a modern software-based configuration and management approaches are identified, and transitioning begins. Applications that cannot follow software-based configuration and management approaches are identified and allowed through exception using a methodical approach.	1. Enterprise-wide guidance on SDC standards are communicated to stakeholders. 2. Components identify applications that can support the SDC approach.	Enterprise best practices support Component efforts in leveraging SDC capabilities.		SDC Resource Authorization Pt2
3.4.4	SDC Resource Authorization Pt2	Application & Workload	Component	Target Level ZT	21.8	Components use approved and validated code/binaries via the Software Bill of Materials (SBOM) process to ensure that applications that can and cannot support the approach are identified. Applications which can support modern Software-Based Configuration and Management (SBCM) approaches are identified and transitioned. Applications that support SBCM have been transitioned to a production/live environment and are in normal operations. Applications which cannot SBCM are identified and allowed through exception using a risk-based approach.	1. Updated applications are deployed in a live and/or production environment. 2. Applications that were marked for retirement and transition have a decommissioned indicator. 3. Applications unable to be updated to an approved binaries/code are marked for retirement and transition plans are created. 4. Identified applications are updated to use approved binaries/code.	Components operationalize validated code and binaries through use in the production environment	SDC Resource Authorization Pt1; Single Authentication; Datacenter Macro-Segmentation	
3.4.5	Enrich Attributes for Resource Authorization Pt1	Application & Workload		Advanced Level ZT	17.6	Initial attributes from various sources, such as User and Entity Activity Monitoring (UEAM), micro-segmentation services, Data Loss Prevention (DLP), and Digital Rights Management (DRM) tools are integrated with the Resource Authorization technology system and policies. Any additional attributes for later integration are identified and planned. Attributes are used to create basic risk posture of users, NPEs and devices allowing for authorization decisions based on the evaluated risk.	1. Most API calls are passing through the Secure API Gateway. 2. Resource Authorization receives data from Analytics Engine. 3. Authorization policies incorporate identified attributes in making authorization decisions. 4. Attributes to be used for initial enrichment are identified and 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
3.4.6	Enrich Attributes for Resource Authorization Pt2	Application & Workload		Advanced Level ZT	17.8	Extended identified attributes are integrated with the resource authorization technology and policy. Confidence scoring system is introduced for identified attributes to create a more advanced method of authorization decision making supporting.	1. Authorization policies incorporate confidence levels in making authorization decisions. 2. Confidence levels for attributes are defined.		Enrich Attributes for Resource Authorization Pt1	
3.4.7	REST API Micro-Segments	Application & Workload		Advanced Level 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 (SDP)controllers and/or Software Defined Networking (SDN) consoles.	1. Approved Enterprise APIs are micro-segmented appropriately.		Automate Application Security & Code Remediation Pt1	

ID#	Activity Name	Pillar	Responsibility	Activity Type	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
3.5.1	Continuous Authorization to Operate (cATO) Pt1	Application & Workload		Advanced Level ZT	15.1	DoD Components utilize automation solutions within the environment to standardize the monitoring of controls and offer the capability to identify deviations. Where appropriate, monitoring and testing is integrated with DevSecOps processes.	1. Controls derivation is standardized and ready for automation. 2. Controls testing is integrated with DevSecOps processes and technology.		Policy Inventory & Development; Build DevSecOps Software Factory Pt2	Continuous Authorization to Operate (cATO) Pt2
3.5.2	Continuous Authorization to Operate (cATO) Pt2	Application & Workload		Advanced Level ZT	21.8	DoD Components fully automate control derivation, testing and monitoring processes. Deviations are automatically tested and resolved using existing cross pillar automation infrastructure. Dashboards are used to monitor the status of authorizations; analytics are integrated with the responsible authorizing officials.	1. Controls testing is fully automated. 2. Integration with standard IR and SOC operations is automated. 3. Control derivation and applicability is fully automated. 4. Dashboards are used to track continuing authorization status.		Continuous Authorization to Operate (cATO) Pt1; Threat Alerting Pt3; Automated Workflow	
4.1.1	Data Analysis	Data	Enterprise and Component	Target Level ZT	17.4	The DoD Enterprise will develop algorithm(s) for components to map data for tagging and labeling, and establish the governing body for oversight. Data at a Component level should be categorized and analyzed by an overseeing governing body.	1. Algorithms are entered into an algorithm registry with appropriate tagging and labeling set by the Enterprise to allow search and retrieval as appropriate (e.g., accommodating data catalog risk alignment). 2. Component data catalog is updated with data types for each application and service based on data classification levels.	Data analysis ensures data protection and reduces risk. All problems have a data analysis algorithm registered in a repository with associated data indicated, and the oversight governance body has awareness that is Visibile, Accessible, Understandable, Linked, Trusted, Interoperable, and Secure (VAULTIS) compliant.		Manual Data Tagging Pt1
4.2.1	Define Data Tagging Standards	Data	Enterprise and Component	Target Level ZT	15.8	Data tagging standard for identifying ZT labels must be defined. The DoD Enterprise works with Components to establish data tagging and classification standards based on industry best practices. Classifications are agreed upon and implemented in processes. Tags are identified as manual and automated for future activities.	1. Enterprise establishes the standard pattern for control vocabulary and how it is managed. 2. Components align to Enterprise standards and begin implementation. 3. Components implement data tagging and labeling standards.	The data dictionary and structure is developed at a broader DoD Enterprise level. ZT specific data attributes are defined in alignment with the Enterprise data dictionary and structure.		Implement Data Tagging & Classification Tools; Manual Data Tagging Pt1; Automated Data Tagging & Support Pt1; Implement Data Tagging & Classification ML Tools
4.2.2	Interoperability Standards	Data	Enterprise and Component	Target Level ZT	14.4	The DoD Enterprise, collaborating with Components, develops interoperability standards methods including mandatory Data Rights Management (DRM) overlays and Protection mechanisms with necessary technologies to enable ZT Target Level functionality.	1. Standard patterns are in place by the Enterprise for appropriate interoperability data sharing.	Interoperability standards for DRM and protection are established and enforced across the Enterprise. These standards are supported by a common language (terms list and scientific definitions) to ensure consistency and clarity. Equal computation outcomes are produced for any rule, and an action agent (enforcement) based on computational results is executed. this unified approach promotes secure, consistent, and compliant data management.		Implement DRM and Protection Tools Pt1
4.2.3	Develop Software Defined Storage (SDS) Policy	Data	Enterprise and Component	Target Level ZT	9.9	The DoD enterprise will work with Components to determine if software define storage (SDS) is in use. DoD Components develop policy and standards based on industry best practices, and evaluate current data storage strategy and technology for implementation of SDS.Components assess their existing data storage strategies and technologies to determine the suitability for implementing SDS. If deemed appropriate, the identified storage technologies are considered for SDS implementation.	1. Enterprise defines and refines minimum attribution requirements for SDS to support Zero Trust enablement. 2. Components assess their existing data storage for SDS implementation considerations.	Ensure holistic approach for SDS security alignment within Components to strengthen access and availability, data protection, and adherence best practices.		Integrate DAAS Access w/SDS Policy Pt1; Integrate Solution & Policy w/Enterprise IDP Pt1; Implement SDS Tool and/or integrate with DRM Tool Pt1
4.3.1	Implement Data Tagging & Classification Tools	Data	Component	Target Level ZT	15.9	DoD Components implement a solution to create new rules, modify existing rules, delete existing rules, check for rule collision, rule deviation, or compound rule inconsistency, and testing of collective rule sets for an outcome. Tools must be adaptable to advanced analytic techniques.	1. Tooling is designed based on Component data tagging efforts that are well-formed with Enterprise-dictated patterns and standards, and are machine readable. 2. Data classification uses data tagging attribution to specify allowed values.	All valid tags can be processed; all invalid tags cannot.	Define Data Tagging Standards	Implement Enforcement Points
4.3.2	Manual Data Tagging Pt1	Data	Component	Target Level ZT	17.6	Components map DoD Enterprise ZT tags to local labeling to meet minimum essential metadata criteria for compliance.	1. Data tagging is conducted at the Component-level with basic attributes.	A standardized data tagging and labeling solution is in place, ensuring all Components comply with ZT principles. Metadata criteria are consistently applied, enhancing data security and access control across the Enterprise.	Data Analysis 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	Data		Advanced Level ZT	16.1	DoD Component specific data level attributes are integrated into the manual data tagging process. DoD Enterprise and Components collaborate to decide which attributes are required to meet ZT Advanced Level functionality. Data level attributes for ZT Advanced Level functionality is standardized across the Enterprise and incorporated.	1. Manual data tagging is expanded to the program/org levels with specific attributes.		Manual Data Tagging Pt1	Enrich Attributes for Resource Authorization Pt1

ID#	Activity Name	Pillar	Responsibility	Activity Type	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
4.3.4	Automated Data Tagging & Support Pt1	Data		Advanced Level ZT	14.1	DoD Components use Data Loss Prevention (DLP), Data Rights Management (DRM), and/or protection solutions to conduct scanning of data repositories. Standardized tags are applied to supported data repositories and data types. Unsupported data repositories and types are identified.	1. Basic automation begins scanning data repositories and applying tags.		Implement Data Tagging & Classification ML Tools	Automated Data Tagging & Support Pt2
4.3.5	Automated Data Tagging & Support Pt2	Data		Advanced Level ZT	38.8	Remaining supported data repositories have basic and extended data tags applied using Machine Learning (ML) and Artificial Intelligence (AI). Extended data tags are applied to existing repositories. Unsupported data repositories and data types are evaluated for decommissioning using a risk-based methodical approach. Approved exceptions utilize manual data tagging approaches with data owners and/or custodians to manage tagging.	1. Full automation of data tagging is completed. 2. 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	Data	Component	Target Level ZT	10.8	DoD Components identify business rules for managing data loss prevention (DLP) enforcement points, such as specific services and user endpoints. Using the established DoD Enterprise cybersecurity incident response standard, DoD Components ensure the appropriate level of detail of data is captured. Additionally, protection, detection, and response use cases are developed to better outline solution coverage.	1. Business rules for access control are established and coordinated with Cyber Operations to support standardized logging for managing DLP enforcement. 2. Standardized logging schema is enforced at the Component-level. 3. Components identify enforcement points.	The right people are allowed to access the right data in the right place at the right time. Data loss prevention rules restrict exfiltration of information from an access control boundary, enhance visibility, and prevent data breaches when aligned with an incident response standard		Comprehensive Data Activity Monitoring
4.4.2	DRM Enforcement Point Logging and Analysis	Data	Component	Target Level ZT	12.6	DoD Components identify business rules for managing the accepted use of the assets managing Data Rights Management (DRM) enforcement points, such as specific services and user endpoints. Using the established DoD Enterprise cybersecurity incident response standard, DoD Components ensure the appropriate detail of data is captured. Additionally, protection, detection, and response use cases are developed to better outline solution coverage.	1. Business rules for managing accepted use of data assets are established and coordinated with Cyber Operations to support standardized logging for managing DRM. 2. Standardized logging schema is enforced at the Component-level. 3. Components identify enforcement points.	Data Rights Management rules restrict the allowed use of information from the access control boundary.		Comprehensive Data Activity Monitoring
4.4.3	File Activity Monitoring Pt1	Data	Component	Target Level ZT	16.8	DoD Components utilize File Monitoring tools to monitor the most critical data classification levels in applications, services, and repositories. Analytics from monitoring is fed into the SIEM with ~~basic~~ data attributes to accomplish ZT Target Level functionality.	1. Data and files of critical data designation are identified and actively monitored. 2. Establish and manage business rules to consume critical data designations and manage outcomes. 3. Integration is in place with monitoring system (e.g., SIEM, XDR).	Files are associated with data assets and objects. File integrity monitoring occurs at the data asset and object levels, allowing for greater visibility and accuracy.		File Activity Monitoring Pt2
4.4.4	File Activity Monitoring Pt2	Data	Component	Target Level ZT	18.9	DoD Components utilize File Monitoring tools to monitor all regulatory protected data (e.g., CUI, PII, PHI, etc.) in applications, services, and repositories. Extended integration is used to send data to appropriate inter/intra-pillar solutions such as Data Loss Prevention, Data Rights Management/Protection and User & Entity Behavior Analytics.	1. Data and files of all regulated designations are identified and actively monitored. 2. Establish and manage business rules to consume regulated designations and manage outcomes.	Components extend regulation to data files and integrations to strengthen data loss prevention, and prevent malicious attacks from spreading.	File Activity Monitoring Pt1	Rule Based Dynamic Access Pt2 Database Activity Monitoring Comprehensive Data Activity Monitoring
4.4.5	Database Activity Monitoring	Data		Advanced Level ZT	18.2	DoD Components procure, implement, and utilize database monitoring solutions to monitor all databases containing regulated data types (e.g., CUI, PII, PHI, etc.). Logs and analytics from the database monitoring solution are provided to the SIEM for monitoring and response. Analytics are utilized in cross pillar activities such as "Enterprise Security Profile Pt 1, Pt 2" and "Real Time Access Decisions" to better direct decision making.	1. Appropriate database are being actively monitored. 2. 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	Data		Advanced Level ZT	27.2	DoD Components expand monitoring of data repositories including databases as appropriate, based on a methodical risk-based approach. Additional data attributes to meet the ZT Advanced Level functionalities are integrated into the analytics for additional integrations.	1. Data activity monitoring mechanisms are integrated to provide a unified view of monitoring across data repositories. 2. Appropriate integrations exist.		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	Data	Component	Target Level ZT	11.7	DoD Components procure and implement DRM and Protection solution(s) as needed, following the DoD Enterprise standard and requirements. Newly implement DRM and protection solution(s) are applied with high-risk data objects.	1. DRM and protection tools are enabled for high-risk data repositories with protections.	No high-risk data object bypasses the compliance requirement.	Interoperability Standards	Implement DRM and Protection Tools Pt2
4.5.2	Implement DRM and Protection Tools Pt2	Data	Component	Target Level ZT	22.0	DRM and protection coverage is expanded to cover all required data objects. Protection mechanisms are automatically managed to meet best practices (e.g., FIPS). Extended data protection attributes are implemented based on the environment classification.	1. DRM and protection tools are enabled for all required repositories.	No data object bypasses the compliance requirement.	Implement DRM and Protection Tools Pt1	

ID#	Activity Name	Pillar	Responsibility	Activity Type	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
4.5.3	DRM Enforcement via Data Tags and Analytics Pt1	Data	Enterprise and Component	Target Level ZT	16.2	DoD Enterprise provides a standard for data access control and protections. Components establish data rights management (DRM) and protection solutions that are used with data tags defined by the data producer. High-risk data objects are identified and monitored with protect and response actions enabled. Data at rest is encrypted and protected (e.g., hardware/object/disk encryption, access control) in repositories.	1. Components DRM utilizes Attribute-Based Access Control standards set by Enterprise. 2. Based on data tags, data is encrypted at rest.	Protections are applied and appropriate access is enforced for each data object.	Manual Data Tagging Pt1	DRM Enforcement via Data Tags and Analytics Pt2
4.5.4	DRM Enforcement via Data Tags and Analytics Pt2	Data		Advanced Level ZT	19.0	Extended data repositories are protected with DRM and protection solutions. DoD Components implement extended data tags applicable to Components versus Enterprise. Data is encrypted in extended repositories using additional tags.	1. All applicable data repositories are protected using DRM. 2. Data is encrypted using extended data tags from the Component level.		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	Data		Advanced Level ZT	23.3	DRM and protection solutions integrate with AI and ML tooling for encryption, rights management, and protection functions.	1. Analytics from ML/AI are integrated with DRM to better automate protections. 2. 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	Data	Component	Target Level ZT	21.2	Data loss prevention (DLP) is aligned to and strengthened by Data Privacy and Protection (DPP). Then through attribution, attributes can be injected that address where data is coming from, its movement across ZT control boundaries, and the invocation of protection measures (e.g., encryption, obfuscation, etc.). Data loss prevention (DLP) solution is deployed to the in-scope enforcement points. It is recommended to start with "monitor-only" and/or "learning" mode limiting impact.- Collaboration with cyber functions should occur with respect to any observed data loss activity.	1. A formal process is established with cybersecurity to share loss activity observations. 2. Identified enforcement points have DLP tool deployed.	DLP solutions are effectively deployed at all identified enforcement points operating in monitor mode with standardized logging. Policies are continuously refined based on DLP results to ensure robust data protection and risk management. Collaborative efforts are established to share insights and strategies, enhancing overall data loss prevention activities across the Enterprise.	Implement Data Tagging & Classification Tools	Process Micro segmentation
4.6.2	DLP Enforcement via Data Tags and Analytics Pt1	Data	Enterprise and Component	Target Level ZT	21.3	Data loss prevention (DLP) solution is updated from monitor only mode to prevention mode. Zero Trust tagging incorporates indicators to facilitate DLP through cooperative cyber enforcement.	1. Enterprise sets the minimum standards for indicators that support cyber enforcement. 2. Components technology is enabled for enforcement.	Support prevention of data loss through development of data attributes that support cyber enforcement of data loss.	Manual Data Tagging Pt1	DLP Enforcement via Data Tags and Analytics Pt2
4.6.3	DLP Enforcement via Data Tags and Analytics Pt2	Data		Advanced Level ZT	19.0	Data Loss Prevention (DLP) solution is updated to include extended data tags based on parallel automation activities.	1. 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	Data		Advanced Level ZT	41.6	Data Loss Prevention (DLP) solution is integrated with automated data tagging techniques, to include any missing enforcement points and tags.	1. 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	Data	Enterprise and Component	Target Level ZT	15.3	Governance mechanisms ensure that component DAAS policy is sufficient for Zero Trust outcomes as established by the SDS policy, if deemed appropriate as established in "4.2.3 Develop Software Defined Storage (SDS) Policy".	1. DAAS access policy is developed with Enterprise and Component support.	A centralized DAAS security approach is implemented across the Enterprise exercising best practices, reducing risk and attack surface area.	Develop Software Defined Storage (SDS) Policy	Integrate DAAS Access w/SDS Policy Pt2
4.7.2	Integrate DAAS Access w/SDS Policy Pt2	Data		Advanced Level ZT	12.6	DoD Components implement the DAAS policy in an automated fashion.	1. 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	Data		Advanced Level ZT	9.2	Newly implemented SDS technology and/or functionalities are integrated with the DAAS policy in a risk-based fashion. A phased approach is taken during implementation to measure results and adjust accordingly.	1. SDS is integrated with DAAS policy functionality. 2. 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	Data	Component	Target Level ZT	13.9	DoD Components integrate attributes associated with access control and data location, and establishes a means for interoperability across DLP, DRM, and storage infrastructure solutions with Enterprise IdP.	1. Component data security solutions are integrated with IdP (e.g. API, LDAP, SAML).	Integrating DLP, DRM, and SDS with the IdP solution to ensure data protection and access is granted to only authenticated and authorized users.	Develop Software Defined Storage (SDS) Policy; Enterprise IDP Pt1	Integrate Solution & Policy w/Enterprise IDP Pt2; Implement SDS Tool and/or integrate with DRM Tool Pt1
4.7.5	Integrate Solution(s) and Policy with Enterprise IDP Pt2	Data		Advanced Level 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 Level functionalities are required for integration.	1. Complete integration with Enterprise IdP and SDS tooling to 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	Data		Advanced Level ZT	17.4	Depending on the need for a Software Defined Storage (SDS) tool, a new solution is implemented, or an existing solution is identified, meeting the functionality requirements to be integrated with DLP, DRM, and ML solutions.	1. 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	Data		Advanced Level ZT	15.3	DoD Components configure the SDS functionality and/or solution to be integrated with the underlying DLP and DRM infrastructure as appropriate. Lower-level integrations enable more effective protection and response.	1. Integrate SDS infrastructure with existing DLP and DRM infrastructure.		Implement SDS Tool and/or Integrate w/DRM Tool Pt1	

ID#	Activity Name	Pillar	Responsibility	Activity Type	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
5.1.1	Define Granular Control Access Rules & Policies Pt1	Network and Environment	Enterprise and Component	Target Level ZT	10.3	The DoD Enterprise working with the Components creates granular network access rules and policies. Associated Concept of Operations (ConOps) are developed in alignment with access policies as well ensure future supportability. Once agreed upon, DoD Components will implement these access policies into existing network technologies (e.g., Next Generation Firewalls, Intrusion Prevention Systems, etc.) to improve initial risk levels and ensure future interoperability.	1. Enterprise provides standardized policy for deployment. 2. Identify Communities of Interest. 3. Components implement access policies according to Enterprise standards and CONOPS.	Provide access control over multiple identities, applications, devices, and traffic levels, reducing the risk of unauthorized accessing and increasing visibility on monitoring for threat response.		Define SDN APIs; Define Granular Control Access Rules & Policies Pt2
5.1.2	Define Granular Control Access Rules & Policies Pt2	Network and Environment	Component	Target Level ZT	8.0	DoD Components utilize data tagging and classification standards to develop data filters for API access to the SDN or alternative networking approach. API Decision Points are formalized within the SDN or alternative network architecture and implemented with non-mission/task critical applications and services.	1. Define data tagging filters for API infrastructure to support interoperability. 2. Enforce authentication for all APIs at the API layer.	Security is enforced at an API level to strengthen authorization and authentication, promote enabling encryption protocols, and support monitoring of malicious behavior at an API level to improve incident response.	Define Granular Control Access Rules & Policies Pt1	
5.2.1	Define SDN APIs	Network and Environment	Enterprise and Component	Target Level ZT	8.3	The DoD Enterprise works with Components to define the necessary APIs and other programmatic interfaces that enable Software Defined Networking (SDN) or alternative networking approach functionalities. These APIs will enable authentication decision point, application delivery control proxy and ssegmentation gateways automation.	1. SDN or alternative networking approach APIs are developed using machine readable patterns and protocols and implemented (per "Standardized API Calls & Schemas Pt1 and Pt2").	SDN or alternative networking approach APIs are standardized and implemented, enabling robust automation of authentication decision points, application delivery control proxies, and segmentation gateways. This standardization ensures consistent and secure SDN or alternative networking approache operations across the Enterprise, enhancing network flexibility, scalability, and security.	Define Granular Control Access Rules & Policies Pt1	Implement SDN Programable Infrastructure
5.2.2	Implement SDN Programable Infrastructure	Network and Environment	Component	Target Level ZT	32.0	Following the API standards, requirements, and SDN API functionalities, DoD Components will implement SoftwareDefined Networking (SDN) or alternative networking approach infrastructure to enable automation tasks. Segmentation gateways and authentication decision points are integrated into the SDN or alternative networking approach infrastructure along with output logging into a standardized repository (e.g., SIEM, Log Analytics) for monitoring and alerting.	1. Components implement application delivery control proxy. 2. Components integrate authentication decision points. 3. Components implement segmentation gateways.	The SDN or alternative networking approach infrastructure is fully implemented across Components, with segmentation gateways and authentication decision points integrated and operational. Comprehensive logging and monitoring are established through SIEM and log analytics, ensuring continuous oversight and rapid response capabilities. The automation of these process enhances network security, efficiency, and compliance with ZT principles.	Define SDN APIs; Standardized API Calls & Schemas Pt1	
5.2.3	Segment Flows into Control, Management, and Data Planes	Network and Environment	Enterprise and Component	Target Level ZT	13.0	Network infrastructure and flows are segmented either physically or logically into separate and distinct control, management, and data planes. Segmentation using IPv6/VLAN approaches is implemented to better organize traffic across data planes. Analytics and NetFlow from the updated infrastructure is automatically fed into Operations Centers and analytics tools.	1. Enterprise provides guidance/policy on segmentation. 2. IPv6/VLAN segmentation is implemented. 3. Enable automated NetOps information reporting. 4. Ensure configuration control across enterprise. 5. Integrated with SIEM/SOAR.	Enterprise provides policy and/or guidance on segmentation. Components further segment network traffic limiting the scope of attack, isolating incidents, and preventing malicious attempts from lateral movement across the network.		B/C/P/S Macro segmentation; Application & Device Micro segmentation
5.2.4	Network Asset Discovery & Optimization	Network and Environment		Advanced Level ZT	30.2	DoD Components automate network asset discovery through the SDN infrastructure, limiting access to devices based on risk-based methodical approaches. Optimization is conducted based on the SDN analytics to improve overall performance along with providing approved access to resources.	1. Technical Refreshment/Technology Evolution. 2. Provide Optimization/Performance Controls.			
5.2.5	Real-Time Access Decisions	Network and Environment		Advanced Level ZT	15.6	SDN infrastructure utilizes cross pillar data sources such as User Activity Monitoring (UAM), Entity Activity Monitoring (EAM), Enterprise security profiles, and more, for real-time access decisions. Machine Learning (ML) is used to assist decision making based on advanced network analytics (i.e., full packet capture, etc.). Policies are consistently implemented across the Enterprise using unified access standards.	1. Analyze SIEM logs with analytics engine to provide real-time policy access decisions. 2. Support sending captured packets, data and network flows, and other specific logs for analytics. 3. Segment end-to-end transport network flows; audit security policies for consistency across Enterprise. 4. 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	Network and Environment	Component	Target Level ZT	17.6	DoD Components implement service-based architectures to restrict lateral movement between public and private components of a solutions architecture. Proxy and/or enforcement checks are integrated with the SDN or alternative networking approach solution(s) based on device attributes and behavior.	1. Establish proxy/enforcement checks of attributes (device, location, data), access and flow (client, tenant, traffic patterns), and Component principles (asset life cycle, compliance, policy).	SDN or alternative networking approach solutions incorporate proxy and enforcement checks based on device attributes and behavior, ensuring robust security. Application delivery control proxies, SIEM logging, UAM, and authentication decision points are integrated and operational. Segmentation gateways are deployed to enhance network security and efficiency.		Implement Micro segmentation; Resource Authorization Pt1; SDC Resource Authorization Pt1

ID#	Activity Name	Pillar	Responsibility	Activity Type	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
5.3.2	B/C/P/S Macro segmentation	Network and Environment	Component	Target Level ZT	18.1	DoD Components implement mission/organization-based macro-segmentation using logical network zones that limit lateral movement. Proxy and/or enforcement checks are integrated with the SDN or alternative networking approach solution(s) based on device attributes and behavior.	1. Establish proxy/enforcement checks of attributes (device, location, data), access and flow (client, tenant, traffic patterns), and Component principles (asset life cycle, compliance, policy). 2. Analyze activities of application specific security stacks for firewall configuration and access policies.	SDN or alternative networking approach solutions incorporate proxy and enforcement checks based on device attributes and behavior, ensuring robust security. Application delivery control proxies, SIEM logging, UAM, and authentication decision points are integrated and operational. Segmentation gateways are deployed to enhance network security and efficiency.	Segment Flows into Control, Management, and Data Planes	
5.4.1	Implement Micro segmentation	Network and Environment	Component	Target Level ZT	17.3	DoD Components implement micro-segmentation infrastructure into SDN or alternative networking approach environment, enabling basic segmentation of service components (e.g., web, app, DB), ports, and protocols. Basic automation is accepted for policy changes, including API decision making. Virtual hosting environments implement micro-segmentation at the host/container-level.	1. Accept automated policy changes. 2. Implement API decision points. 3. Implement distributed NGF/micro-FW/endpoint agent in virtual hosting environment.	Automated policy changes and API decision-making processes are established, enhancing the agility and security of the infrastructure. Virtual hosting environments employ micro-segmentation at the host/container level providing robust security controls and improving overall management efficiency. the infrastructure includes integrated application delivery control proxies, SIEM logging, UAM, authentication decision points, and segmentation gateways, ensuring comprehensive security and monitoring capabilities.	Datacenter Macro segmentation	Application & Device Micro segmentation
5.4.2	Application & Device Micro segmentation	Network and Environment	Component	Target Level ZT	17.9	DoD Components utilize Software Defined Networking (SDN) or alternative networking approach solution(s) to establish infrastructure meeting the ZT Target Level functionalities - i.e., logical network zones; Role, Attribute, and Condition-Based Access Control for Users and Devices, Privileged Access Management (PAM) services for network resources, and policy-based control on API access.	1. Assign Role, Attribute, and Condition-Based Access Control to Users & Devices. 2. Provide PAM services. 3. Limit Access on a Per-Identity basis for users and devices. 4. Create logical network zones. 5. Support policy control via REST API.	SDN or alternative networking approach infrastructure is established across DoD Components, providing robust Role, Attribute, and Condition-Based Access Control for PEs and NPEs. PAM services are in place for network resources. Logical network zones are created, and policy-based controls are enforced on API access via REST APIs. This ensures secure and controlled access management, enhancing the overall security posture.	Segment Flows into Control, Management, and Data Planes; Implement Micro segmentation	Enrich Attributes for Resource Authorization Pt1
5.4.3	Process Micro segmentation	Network and Environment		Advanced Level ZT	20.3	DoD Components utilize existing micro-segmentation and SDN automation infrastructure enabling process micro-segmentation. Host-level processes are segmented based on security policies and access is granted using real-time access decision making.	1. Segment host-level processes for security policies. 2. Support real-time access decisions and policy changes. 3. Support offload of logs for analytics and automation. 4. Support dynamic deployment of segmentation policy.		Implement Enforcement Points	
5.4.4	Protect Data In Transit	Network and Environment	Enterprise and Component	Target Level ZT	9.1	Based on the data flow mappings and monitoring standards provided by DoD Enterprise, policies are enabled by DoD Components to mandate protection of data in transit. Common use cases, such as Coalition Information Sharing, sharing across system boundaries and protection across architectural components, are included in protection policies.	1. Enterprise guidance is provided on protecting Data In Transit. 2. Protect data in transit during Coalition Information Sharing. 3. Protect data in transit across system high boundaries. 4.Integrate data in transit protection across architecture components.	Policies are effectively implemented to protect data in transit during coalition information sharing across system high boundaries, and within various architectural components. Data in transit is securely encrypted and monitored ensuring ZT.		
6.1.1	Policy Inventory & Development	Automation and Orchestration	Enterprise and Component	Target Level ZT	9.8	The DoD Enterprise works with Components to catalog and inventory existing cybersecurity policies and standards. Policies are updated and created in cross-pillar activities as needed to meet critical ZT Target Level functionality.	1. Component policies have been collected in reference to applicable compliance and risk (e.g., RMF, NIST). 2. Policies have been reviewed for missing Pillars and Capabilities by Enterprise per the ZTRA. 3. Enterprise and Components make updates to missing areas of policies to meet the capabilities per the ZTRA.	Policies are aligned to support interoperability and enable ZT functionality.		Continuous Authorization to Operate (cATO) Pt1
6.1.2	Organization Access Profile	Automation and Orchestration	Enterprise and Component	Target Level ZT	19.4	DoD Components develop access profile rules for mission/task and non-mission/task DAAS access using the data from the User, Data, Network & Environment, and Device pillars. The DoD Enterprise works with the Components to develop an Enterprise security profile rules using the existing Component security profiles to create a common access approach to DAAS. A phased approach can be used by Components to limit risk to mission/task critical DAAS access once the security profile(s) are created.	1. Component scoped profile rules are created to determine access to DAAS using capabilities from User, Data, Network & Environment, and Device pillars. 2. Initial Enterprise profile rules for access standard is developed for access to DAAS. 3. When possible, Component profile(s) utilize Enterprise available services in the User, Data, Network & Environment, and Device pillars. 4. Component mission/task critical profile rules are created.	The patterns of behavior are established for what outcomes are needed for access control at the Component level.		Enterprise Security Profile Pt1

ID#	Activity Name	Pillar	Responsibility	Activity Type	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
6.1.3	Enterprise Security Profile Pt1	Automation and Orchestration	Enterprise and Component	Target Level ZT	16.0	Enterprise security profile rules covers the User, Data, Network & Environment, and Device pillars initially. Existing Component security profile rules are integrated for non-mission/task DAAS access following an iterative approach to tuning access.	1. Enterprise profile rules are created to access DAAS using capabilities from User, Data, Network & Environment, and Device pillars. 2. Component profile rules are integrated with the Enterprise profile rules using a standardized approach. 3. Service catalog and/or CMDB exists with ZT components; at a minimum PDP(s), PEP(s), and PIP(s) details inventoried.	The patterns of behavior are established for necessary outcomes of access control at the Enterprise level.	Organization Access Profile	Enterprise Security Profile Pt2
6.1.4	Enterprise Security Profile Pt2	Automation and Orchestration		Advanced Level ZT	12.5	The minimum number of Enterprise security profile(s) exist that grant access to the widest range of DAAS within the DoD Compontents. Mission/task Component profiles are integrated with the Enterprise security profile(s) and exceptions are managed in a risk-based methodical approach.	1. Enterprise security profile(s) have been reduced and simplified to support widest array of access to DAAS. 2. Mission/Task Critical profile(s) have been integrated and supported Component profiles are considered the exception.		Enterprise Security Profile Pt1	Real-Time Access Decisions; AI-enabled Dynamic Access Control
6.2.1	Task Automation Analysis	Automation and Orchestration	Component	Target Level ZT	6.3	DoD Components identify and enumerate all task activities that can be executed both manually and in an automated fashion. Task activities are organized into automated and manual categories. Manual activities are analyzed for retirement.	1. Automatable tasks are identified. 2. Tasks are enumerated. 3. Components create process flow of all cybersecurity defense automations tasks developed with an independent audit process before operational implementation.	Components optimize mission-critical processes with automation, reducing the time and resources spent, increasing accuracy (limiting human error) when validated, and supporting incident response.		
6.2.2	Enterprise Integration & Workflow Provisioning Pt1	Automation and Orchestration	Enterprise and Component	Target Level ZT	23.4	The DoD Enterprise establishes baseline integration and interoperability within the Security Orchestration, Automation, and Response (SOAR) solution required to enable ZTA Target Level functionality, where actionable and relevant information resides. DoD Components identify instrument, integration, and interoperability points and prioritization-per the Enterprise baseline. The necessary integrations in User, Device, Application & Workload, Network & Environment, and Device pillars to automate IR functions are completed.	1. DoD Enterprise establishes baseline integration and interoperability with SOAR to enable ZT Target Level functionality. 2. Components identify key integrations. 3. Components implement Enterprise integration and interoperability for critical services. 4. Components identify recovery and protection requirements.	Critical integrations occur to meet key services and enable recovery and protection capabilities.		Enterprise Integration & Workflow Provisioning Pt2
6.2.3	Enterprise Integration & Workflow Provisioning Pt2	Automation and Orchestration		Advanced Level ZT	12.7	DoD Components integrate remaining services to meet baseline requirements and ZT Advanced Level functionality requirements. Service provisioning is integrated and automated into workflows, where required, meeting ZT Target Level functionalities.	1. Services identified. 2. Service provisioning is implemented.		Enterprise Integration & Workflow Provisioning Pt1	Automated Workflow
6.3.1	Implement Data Tagging & Classification ML Tools	Automation and Orchestration	Component	Target Level ZT	16.0	DoD Components utilize existing Data Tagging and Classification standards and requirements to integrate Machine Learning (ML) solution(s)/capability as needed. ML solution(s) is implemented by Components, and existing tagged and classified data repositories are used to establish baselines. ML solution(s) applies data tags in a supervised approach to continually improve analysis.	1. Components implement ML capabilities with data tagging and classification.	Machine learning solution is acquired, trained, and implemented in accordance with DoD established Data Tagging and Classification tools. Machines are trained on a high-quality subset of data developed under activity 4.3.1 with human oversight and assessment.	Define Data Tagging Standards	Automated Data Tagging & Support Pt2
6.4.1	Implement AI automation tools	Automation and Orchestration		Advanced Level ZT	25.7	DoD Components identify areas of improvement based on existing Machine Learning (ML) techniques for Artificial Intelligence (AI). AI solutions are identified, procured, and implemented using the identified areas as requirements.	1. Develop AI tool requirements. 2. Procure and implement AI tools.			Automated Workflow
6.4.2	AI Driven by Analytics decides A&O modifications	Automation and Orchestration		Advanced Level ZT	42.0	DoD Components, utilizing existing Machine Learning (ML) functions, implement and use AI technology, such as neural networks, to drive automation and orchestration decisions. Decision making is moved to AI as much as possible, freeing up human staff for other efforts. Utilizing historical patterns, AI will make anticipatory changes in the environment to better reduce risk.	1. AI is able to make changes to automated workflow activities.			
6.5.1	Response Automation Analysis	Automation and Orchestration	Component	Target Level ZT	9.0	DoD Components identify and enumerate all response activities that are executed both manually and in an automated fashion. Response activities are organized into automated and manual categories.	1. Automatable response activities are identified. 2. Response activities are enumerated.	Components optimize response processes with automation, improving the response time for true positives and supporting a better awareness and understanding of security incidents.		

ID#	Activity Name	Pillar	Responsibility	Activity Type	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
6.5.2	Implement SOAR Tools	Automation and Orchestration	Enterprise and Component	Target Level ZT	14.9	DoD Enterprise, working with Components, develops a standard set of requirements for Security Orchestration, Automation, and Response (SOAR) tooling to enable ZT Target Level functionallity. DoD Components use approved requirements to procure and implement a SOAR solutions. Iinfrastructure integrations for future SOAR functionality is completed.	1. Enterprise develops requirements for SOAR tools. 2. Components procure SOAR tools. 3. Components develop Implementation Plan (e.g., Integration Points, Incident Response, Architecture, Interoperability, Scalability, etc.) for SOAR. 4. Complete full implementation of SOAR.	Components conduct appropriate planning to ensure effective implementation of a SOAR tool with relevant connections and interoperability.	Standardized API Calls & Schemas Pt1; Workflow Enrichment Pt1	
6.5.3	Implement Playbooks	Automation and Orchestration		Advanced Level ZT	14.0	DoD Components review all existing playbooks to identify for future automation. Existing manual and automated processes missing playbooks have playbooks developed. Playbooks are prioritized for automation to be integrated with the "Automated Workflows" activities covering critical processes. Manual processes without playbooks are authorized using a risk-based methodical approach.	1. Automate playbooks based on automated workflows capability. 2. Manual Playbooks are developed and implemented.			
6.6.1	Tool Compliance Analysis	Automation and Orchestration	Component	Target Level ZT	7.3	Automation and Orchestration tooling and solutions are analyzed for compliance and capabilities based on the DoD Enterprise API machine-readable patterns and protocols.	1. Components API status is determined to be compliant or non-compliant to Enterprise API standards.	Ensure tools includes standardized API security with the proper protocols and capabilities to monitor, control access, and interoperate with other pillars.		
6.6.2	Standardized API Calls & Schemas Pt1	Automation and Orchestration	Enterprise and Component	Target Level ZT	13.6	The DoD Enterprise works with components to establish an API standard (or equivalent automated interchange mechanism), which at least outlines the approved patterns and protocols. DoD Components identify existing APIs and update to the standard.	1. API Standard (or equivalent automated interchange mechanism) is established with Component commitment. 2. Automated pattern and protocol services are implemented.	Existing APIs are assessed against automated pattern and protocol services.		Implement SDN Programable Infrastructure; Implement SOAR Tools; Standardized API Calls & Schemas Pt2
6.6.3	Standardized API Calls & Schemas Pt2	Automation and Orchestration	Component	Target Level ZT	14.2	DoD Components will ensure that all ZT applications/services (i.e., PEP, PDP, PIP) adopt the API standard. Information Systems required to follow ZT Target or Advanced Levels prioritize integration with the API standard to simplify automation.	1. Components implement API Standard for all ZT Applications/Services (i.e., PEP, PDP, PIP).	For each ZT service edge, Components will have an automated pattern and protocol service.	Standardized API Calls & Schemas Pt1	
6.7.1	Workflow Enrichment Pt1	Automation and Orchestration	Enterprise and Component	Target Level ZT	7.3	DoD Enterprise works with Components to establish cybersecurity incident response guidance using industry best practices, such as NIST and a list of approved threat data sources as specified in "Cyber Threat Intelligence Program Pt 1". DoD Components enable workflows for security events using internal context, past threat events, and other threat intelligence. Approved external sources of enrichment are identified for future integration. These workflows are used to determine incident response procedures.	1. Threat events are identified utilizing DoD Enterprise guidance and best practice. 2. Components establish workflows for threat events and include enrichment from approved sources and business/mission context.	Component workflows provide security teams with the intelligence needed to better detect, investigate, and respond to incidents more effectively.		Implement SOAR Tools; Workflow Enrichment Pt2
6.7.2	Workflow Enrichment Pt2	Automation and Orchestration	Component	Target Level ZT	9.1	DoD Components identify and establish extended workflows for additional incident response types in alignment with the activity "Threat Alerting Pt 2". Initial enrichment data sources are used for existing workflows. Additional enrichment sources (e.g., UAM, UEBA, profiles, and baselines) are identified for future integrations.	1. Workflows for advanced threat events are developed by Components. 2. Advanced threat events are identified.	Component workflows provide security teams with the intelligence needed to better detect, investigate, and respond to incidents more effectively.	Workflow Enrichment Pt1	Workflow Enrichment Pt3
6.7.3	Workflow Enrichment Pt3	Automation and Orchestration		Advanced Level ZT	12.4	DoD Components use enrichment data sources on basic and extended threat response workflows.	1. Enrichment data has been identified. 2. Enrichment data is integrated into workflows.		Workflow Enrichment Pt2	Automated Workflow
6.7.4	Automated Workflow	Automation and Orchestration		Advanced Level ZT	14.4	DoD Components focus on automating Security Orchestration, Automation, and Response (SOAR) functions and playbooks. Manual processes within security operations are identified and fully automated as possible. Remaining manual processes are decommissioned when possible or marked for exception using a risk-based approach.	1. Workflow processes are fully automated. 2. Manual processes have been identified. 3. 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
7.1.1	Scale Considerations	Visibility and Analytics	Component	Target Level ZT	11.6	DoD Components conduct analysis to determine current and future scaling needs for monitoring, detection, and response. This requires a prioritization plan aligned with Component business/mission considerations and associated risk alignment. Scaling is analyzed following common industry best practice and aligns with ZT Pillar requirements. The team works with existing Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) groups to determine distributed environment needs in emergencies and Component growth.	1. Evaluate opportunities for scaling (e.g., infrastructure sizing, bandwidth capacity, distributed environments) across the different pillars as it applies to visibility and analytics outcomes. 2. Create or utilize existing governance structure to operationalize the strategy.	Analyze scaling needs for monitoring, detection, and response, aligning with business considerations, risk, industry best practices, and ZT Pillar requirements, while collaborating with BCP and DRP groups for distributed environment needs during emergencies and growth.		

ID#	Activity Name	Pillar	Responsibility	Activity Type	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
7.1.2	Log Parsing	Visibility and Analytics	Enterprise and Component	Target Level ZT	6.3	DoD Components identify and prioritize log and flow sources (e.g., firewalls, Endpoint Detection & Response, Active Directory, switches, routers, etc.) and develop a plan for collection of high-priority logs first, then low-priority. An open industry-standard log format is agreed upon at the DoD Enterprise level with the Components, and implemented in future procurement requirements. Existing solutions and technologies are migrated to this format on a continual basis.	1. Enterprise standardized log formats. 2. Components implement rules developed for each log format.	Components filter and forward all applicable log events to the SIEM.		Implement Analytics Tools; Asset ID & Alert Correlation
7.1.3	Log Analysis	Visibility and Analytics	Enterprise and Component	Target Level ZT	10.3	Enterprise develops common user and device activities. Components identify and prioritize activities based on risk. Events/flows deemed the most simplistic and risky have analytics created using different data sources, such as logs. Trends and patterns are developed over longer periods of time.	1. Identify activities to analyze. 2. Determine risk level per events/flows.	Components utilize logs to develop risk level for each user and device.		Establish User Baseline Behavior User/Device Baselines
7.2.1	Threat Alerting Pt1	Visibility and Analytics	Component	Target Level ZT	7.5	DoD Components utilize existing Security Information and Event Management (SIEM) solution to develop rules and alerts for common threat events (e.g., malware, phishing, etc.) Alerts and/or rule triggers are fed into the parallel “Asset ID & Alert Correlation” activity to begin automation of responses.	1. Rules developed for Component-derived threat correlation. 2. Rules developed for asset ID-based responses.	Components augment SIEM with threat data developed from incident response analysis.		Threat Alerting Pt2; Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt1
7.2.2	Threat Alerting Pt2	Visibility and Analytics	Component	Target Level ZT	16.5	DoD Components expand threat alerting in the Security Information and Event Management (SIEM) solution to include Cyber Threat Intelligence (CTI) data feeds. Deviation and anomaly rules are developed in the SIEM to detect advanced threats.	1. Rules developed for advanced threat correlation (e.g., behavioral, baseline deviation).	Components augment SIEM with threat data from CTI feeds.	Threat Alerting Pt1; Cyber Threat Intelligence Program Pt1	Threat Alerting Pt3
7.2.3	Threat Alerting Pt3	Visibility and Analytics		Advanced Level 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.	1. Identify triggering anomalous events. 2. 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	Visibility and Analytics	Component	Target Level ZT	10.2	All assets in SIEM are identified and correlated to alerts in order to provide security teams with accurate and detailed information. This information contributes to the incident response speed. Asset ID's also allow better visibility while preforming vulnerability assessments.	1. Identify and provide as much detail as needed for identification of all assets in SIEM, including correlation to alerts in support of "Threat Alerting Pt1".	Security is able to quickly identify assets in relation to threat events in a way that betters supports incident response.	Log Parsing	
7.2.5	User/Device Baselines	Visibility and Analytics	Component	Target Level ZT	13.0	DoD Components develop a subject/attribute baseline approach based on typical pattern and behavior in activity "Establish User Baseline Behavior". This approach will serve as a benchmark for security when identifying and responding to abnormal or malicious activity.	1. Components identify a subject/attribute baseline approach.	Components can utilize baseline approach to build profiles in activity "Baseline and Profiling Pt 1".	Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling; Log Analysis; Establish User Baseline Behavior Pattern	User Activity Monitoring Pt1; Entity Activity Monitoring Pt1
7.3.1	Implement Analytics Tools	Visibility and Analytics	Enterprise and Component	Target Level ZT	12.1	The DOD Enterprise provides minimum requirements for analytics tool capabilities to analyze data across all ZT pillars. Components procure and implement an analytics tool in order to provide actionable insights and intelligence.	1. Enterprise develops requirements for analytic environment. 2. Components procure and implement analytic tools.	Analytics tools provide intelligence and guidance to security teams in order to make improvements on threat monitoring and response.	Log Parsing	
7.3.2	Establish User Baseline Behavior	Visibility and Analytics	Component	Target Level ZT	13.8	Utilizing the analytics tools implemented, subject behavior patterns are analyzed to identify patterns and deviations from normality. Techniques in analytics involve machine learning and UEBA.	1. Establish subject behavior patterns in order to differentiate normality/abnormality. 2. Identify opportunities for ML usage in analytics.	Patterns established will provide Components with decision making for user/device baselines.	Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling; Log Analysis	User/Device Baselines; Baseline & Risk Profiling Pt1
7.4.1	Baseline & Profiling Pt1	Visibility and Analytics	Component	Target Level ZT	12.3	Utilizing the baselines developed in the "User/Device Baselines" activity, threat profiles are created to assess the level of risk for individual subjects associated to the overall Component security. Profiles should be integrated into the "Orginization Access Profile" activity for decision making.	1. Identify subject/attribute threat profiles. 2. Develop analytics to detect changing threat conditions.	Components are able create risk profiles to mitigate compromised accounts, suspicious activity, and insider threats.	Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling; Log Analysis; Establish User Behavior Pattern	Baseline & Profiling Pt2

ID#	Activity Name	Pillar	Responsibility	Activity Type	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
7.4.2	Baseline & Profiling Pt2	Visibility and Analytics		Advanced Level ZT	22.7	DoD Components expand baselines and profiles to include unmanaged and non-standard device types, including Internet of Things (IoT) and Operational Technology (OT), through data output monitoring. These devices are again profiled based on standardized attributes and use cases. Analytics are updated to consider the new baselines and profiles, accordingly enabling further detections and response. Specific risky users and devices are automatically prioritized for increased monitoring based on risk. Detection and response are integrated with cross pillar functionalities.	1. Add threat profiles for IoT and OT devices. 2. Develop and extend analytics. 3. Extend threat profiles to individual users and devices.		Baseline & Profiling Pt1	
7.4.3	UEBA Baseline Support Pt 1	Visibility and Analytics		Advanced Level ZT	6.3	User & Entity Behavior Analytics (UEBA) within DoD Components expands monitoring to advanced analytics such as Machine Learning (ML). These results are in turn reviewed and provided back into ML algorithms to improve detection and response.	1. 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	Visibility and Analytics		Advanced Level ZT	6.3	User & Entity Behavior Analytics (UEBA) within DoD Components completes it expansion by using traditional and Machine Learning (ML) based results to be provided to Artificial Intelligence (AI) algorithms. AI based detections are supervised, but ultimately, using advanced techniques such as neural networks, UEBA operators are not part of the learning process.	1. Implement ML-based analytics to detect anomalies.		UEBA Baseline Support Pt1	
7.5.1	Cyber Threat Intelligence Program Pt1	Visibility and Analytics	Enterprise and Component	Target Level ZT	9.9	The DoD Enterprise works with Components to develop a Cyber Threat Intelligence (CTI) program policy, standard, and process. Components utilize this documentation to develop organizational CTI teams with key mission/task stakeholders. CTI teams gather intelligence from common data feeds across ZT Pillars and aggregate all intelligence to a centralized repository (e.g. SIEM).	1. DoD Enterprise develops a Cyber Threat Intelligence (CTI) program policy. 2. Component CTI team is in place with critical stakeholders. 3. Common CTI feeds are being utilized by SIEM for monitoring. 4. Integration points exist with device and network PEP/PDP (e.g., NGAV, NGFW, NG-IPS) are built at appropriate integration points across each pillar.	Component CTI teams are established in accordance with Enterprise policy and have integrated CTI data feeds in their SEIM(s).		Cyber Threat Intelligence Program Pt2; Threat Alerting Pt 2
7.5.2	Cyber Threat Intelligence Program Pt2	Visibility and Analytics	Component	Target Level ZT	19.5	DoD Components expand their Cyber Threat Intelligence (CTI) teams to include new stakeholders as appropriate. Existing and authenticated, private and controlled threat intelligence is analyzed, and appropriate actions and controls are enforced across ZT Pillars. CTI Program adapts strategy over time with expansion of threat intelligence developed in solutions and program maturity.	1. Component Cyber Threat Intelligence team is in place with extended stakeholders as appropriate. 2. Integration is in place for extended enforcement points across ZT Pillars (e.g., UEBA,UAM).	Component CTI teams utilize threat intelligence data to support control enforcement to a greater extent throughout the organization via tooling.	Cyber Threat Intelligence Program Pt1	
7.6.1	AI-enabled Network Access	Visibility and Analytics		Advanced Level ZT	27.8	DoD Components utilize SDN infrastructure and Enterprise security profiles to enable Artificial Intelligence (AI)/Machine Learning (ML) driven network access. Analytics from previous activities are used to teach the AI/ML algorithms; improving decision making.	1. 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	Visibility and Analytics		Advanced Level ZT	24.4	DoD Components utilize previous rule-based dynamic access to teach Artificial Intelligence (AI)/Machine Learning (ML) algorithms to make access decisions to resources. The “AI-enabled Network Access” activity algorithms are updated to enable broader decision making to all DAAS.	1. JIT/JEA are integrated with AI; Access is AI driven based on environment analytics.		Continuous Authentication Pt2; AI-enabled Network Access	