ID#	Activity Name	Pillar	Responsibility	Phase	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 lifecycle 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	The DoD ICAM governance establishes a set of user attributes for authentication and authorization. These are integrated with the "Enterprise Identity Life-Cycle Management Pt1" activity process for a complete enterprise standard. The Enterprise Identity, Credential and Access Management (ICAM) solution are enabled for -adding/updating attributes within the solution to betters support identity federation. Remaining Privileged Access Management (PAM) activities are approved and tailored as specified by the roles.	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 network/system boundary. 4. Component ICAM implementation obtain authoritative information about personnel (i.e. attributes, and entitlements) from a central attribute source once. available, or from other DoD Components using standard profiles otherwise.	Authoritative attributes requiired to implement conditional user access into applications are available to support privleged 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 access and Just-Enough-Administration methods.	1. Access to 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
1.3.1	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 (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 enabling key pairs to be signed by the trusted root certificate authorities. 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 multifactor 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). 5. For access to low-risk resources (e.g. personal PII and publicly released information), utilize alternative two-step, two-factor authentication using software authenticators (i.e., Mobile Connect, Yubico, Okta Verify).	Critical applications are identified and use MFA in alignment with a federated IdP solution.		
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 support all critical privileged use cases. Application/Service integration points are identified to determine status of support for the PAM solution. Applications/Services that easily integrate with PAM solution are transitioned over to using 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 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 Mitigate Privileged Users Pt2

ID#	Activity Name	Pillar	Responsibility	Phase	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
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 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 Mitigate Privileged Users Pt1	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 Lifecycle Process.	Establishing a comprehensive and efficient process that ensures the accurate and secure management of user identities throughout their entire lifecycle 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 the DoD Components. DoD Components implement the Enterprise Lifecycle 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 lifecycle processes. 2. Integrated with Enterprise ICAM process and tools.	Implementing consistent and well-defined processes and controls for managing the maximum number of identities in the lifecycle.	Organization Identity Life-cycle Management	Enterprise Identity Life-cycle 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, detect anomalies, and protect against unauthorized access.		Establish User Baseline Behavior; User/Device Baselines Alternative Flexible MFA PT2
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 reduced permissions 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 permissions levels are implemented. 3. Applications/services have reviewed/audited all privileged users and removed those users who do not need that level of access. 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 the network, systems, and applications. 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 but other period-based analytics can be used to mandate re-authentication of user sessions.	1. Authentication implemented multiple times per session based on security attributes and criticality of the data, user, app, system, and source user location.	Authentication occurs per the requirement and standard.	Single Authentication	Continuous Authentication Pt1; AI-enabled Network Access
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’s off. Components’ PKI Certificated Authorities are integrated with the Enterprise PKI. An Enterprise Identity Provider platform is implemented. The Identity Provider 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 NPE &PE 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 Platform. 4. Enterprise wide Identity Provider 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	Phase	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
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. Device attributes tracked in the inventory.	1. Inventory of authorized and approved devices is created per Component w/ owners. 2. Determine and implement tools to gauge device health.	A comprehensive inventory of authorized and approved devices with designated owners, and to implement effective tools for monitoring and assessing device health.		

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. Additional other Non-Person Entities (NPEs) (e.g., web servers, network devices, routers, applications) that support x509 certificates are assigned 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/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, are provided an exception based on risk analysis, or are marked for retirement as part of the enterprise lifecycle management plan.		Enterprise IDP Pt2
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 ZTA Target functionalities.	1. C2C is enforced at the Component level for all environments. 2. All Mandated devices 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
2.3.3	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. FIMs 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 later movement, expanding the capabilities and response than traditional executable containment. Both FIMS and Application containment continues the development of the device, data, and application pillar.	1. App 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 in place.		
2.3.4	Integrate NextGen AV Tools with C2C	Device	Component	Target Level ZT	18.5	DoD Components procure and implements an Endpoint Protection Platform. EPP should have the capabilities to use advanced analytics (e.g., artificial intelligence, behavioral detection, machine learning) and mitigate exploits so zero days, signatureless, fileless, provide Network Access Control and known/unknown threats can be prevented. 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. Endpoint Protection Platform (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.		Implement C2C/Compliance Based Network Authorization 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 to tailor pertaining to specific environment. DoD Components will block all unmanaged remote and local device access to resources. Compliant managed devices are provided risk based methodical access following ZTA target level concepts.	1. Enterprise set standards for deny device by default policy. 2. Components will block unmanaged device remotely/locally. 3. Access is enabled strictly for compliant devices remotely/locally following "deny device by default policy" approach.	All device access is authorized/verified/compliant and unauthorized/unmanaged 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 Devices and IoT. 2. Component BYOD and IOT device permissions are baselined and integrated with Enterprise IDP.	Components establish a foundation for risk-based access control by for BYOD and IoT with dynamic permissions		Implement C2C/Compliance Based Network Authorization Pt1; Managed and Full BYOD & IOT Support Pt1
2.5.1	Implement Asset, Vulnerability and Patch Management Tools	Device	Component	Target Level ZT	18.4	DoD Components implement solution(s) for managing assets/devices 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

ID#	Activity Name	Pillar	Responsibility	Phase	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
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 and 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 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. DoD Components migrate the manual device inventory to an automated approach using a Enterprise Device Management solution. Approved devices are able to be managed regardless of location. Devices part of critical services are mandated to be managed by the Enterprise Device Management 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 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 a 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 functionality and is sending data to the Comply to Connection solution for expanded device and user checks.	1. Endpoint Detection & Response 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 can't be detected 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) & 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 Component 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 should be in alignment with C2C. XDR capabilities would either supplement or replace EDR implementation activity . 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 threat landscape allowing for coordinated response, automation and orchestration when responding to threats.	Implement Endpoint Detection & Response (EDR) Tools & Integrate w/ C2C; Threat Alerting Pt1	Implement Extended Detection & Response (XDR) & Integrate w/ C2C Pt 2
3.1.1	Application/Code Identification	Applications and 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. Each Component will track the supportability (i.e., active, legacy, etc.) hosted location (i.e., cloud, on-premise, 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	Applications and 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 which includes requirements gathering, design, development, testing and deploying.	1. Developed security best practices for DevSecOps and CI/CD Pipeline. 2. Vulnerability management is integrated into the CI/CD pipeline.	Implementing consistent and well-defined processes and controls for DevSecOps.		Build DevSecOps Software Factory Pt2 Automate Application Security & Code Remediation Pt1
3.2.2	Build DevSecOps Software Factory Pt2	Applications and 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. Development of applications adopts the use of the CI/CD pipeline. 3. Continual validation process/technology is implemented and in use (see "Continual Validation" activity). 4. Development of applications 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 (carto) Pt1

ID#	Activity Name	Pillar	Responsibility	Phase	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
3.2.3	Automate Application Security & Code Remediation Pt1	Applications and 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 appropriate.	1. Enterprise sets standardized approach to application security including code remediation. 2. Secure API Gateway is operational and majority of API calls are passing through 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
3.3.1	Approved Binaries/Code	Applications and Workload	Enterprise	Target Level ZT	23.4	The DoD Enterprise uses best practice approaches to manage approved binaries and code in a methodical approach. These approaches will include supplier sourcing risk management, approved repository usage, bill of materials supply chain risk management, and industry standard vulnerability management.	1. Supplier sourcing risk evaluated and identified for approved sources. 2. Repository and update channel established for use by development teams. 3. Bill of Materials is created for applications to identify source, supportability and risk posture. 4. Industry standard (DIB) 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	Applications and Workload	Enterprise and Component	Target Level ZT	7.8	The DoD Enterprise works with Components to establish and manage a Vulnerability Management program. The developed program includes at a minimum the tracking and management of public vulnerabilities based on DoD applications/services. Components establish a vulnerability management team with key stakeholders where vulnerabilities are discussed and managed following the Enterprise policy and standards.	1. Components establish A vulnerability management governance team w/ appropriate stakeholder membership. 2. Enterprise provides a Vulnerability Management policy and standard for minimum tracking and management of public vulnerabilities based on DoD application/services.	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	Applications and 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/operated services both publicly and privately accessible. DoD Components expand the vulnerability management program to track and manage closed vulnerability repositories such as DIB, CERT, and others.	1. Components Utilize Controlled (e.g., DIB, 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	Applications and 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 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 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.		
3.4.1	Resource Authorization Pt1	Applications and 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 for external facing applications/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 for external facing applications and services. 3. DoD Enterprise-Wide Interoperability Guidance 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

ID#	Activity Name	Pillar	Responsibility	Phase	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
3.4.2	Resource Authorization Pt2	Applications and Workload	Component	Target Level ZT	20.6	Policy enforcements and decisions are used for all possible applications/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. 2. Applications 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	Applications and Workload	Enterprise and Component	Target Level ZT	31.1	The DoD Enterprise provides best practices for code based compute management (i.e., Software Defined Compute). 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 which can support a modern software-based configuration and management approaches are identified and transitioning begins. Applications which cannot follow software-based configuration and management approaches are identified and allowed through exception using a methodical approach.	1. Enterprise-wide Guidance on SDC standards are communicated to stakeholders. 2. Components identify applications that can support SDC approach.	Enterprise best practices support component efforts in leveraging SDC capabilities.		SDC Resource Authorization Pt2
3.4.4	SDC Resource Authorization Pt2	Applications and Workload	Component	Target Level ZT	21.8	Components use approved and validated code/binaries via SBOM process to ensure that applications are identified which can and that cannot support the approach. Applications which can support modern software-based configuration and management approaches are identified and transitioned. Applications-that support software-based configuration and management have been transitioned to a production/live environment and are in normal operations. Applications which cannot support software-based configuration and management 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 use approved binaries/code are marked for retirement and transition plans are created. 4. Identified applications without use approved and process 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	
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 overseeing governing body.	1. Algorithms are entered into an algorithm registry with appropriate tagging and labeling set by 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 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 level. ZT-Specific data attributes are defined in alignment with the DoD 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 the components develops interoperability standards methods including mandatory Data Rights Management (DRM) overlays and Protection mechanisms with necessary technologies to enable ZT target 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 working with organizations to establish 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 provides minimum attribution required for SDS is created and refined for Zero Trust enablement. 2. Components assess their existing data storage for SDS implementation considerations.	Ensure holistic approach for SDS security alignment within the 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

ID#	Activity Name	Pillar	Responsibility	Phase	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
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 use 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 ZT 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
4.4.1	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 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 component levels. 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 digital asset 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 component levels 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 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
4.5.1	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 implemented 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	
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 in repositories.-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
4.6.1	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 (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 point 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

ID#	Activity Name	Pillar	Responsibility	Phase	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
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
4.7.1	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 w/ enterprise and component level support.	A centralized DAAS security approach is implemented across the department exercising best practices, reducing risk and attack surface area.	Develop Software Defined Storage (SDS) Policy; ~~Enterprise IDP Pt1~~	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 create 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
5.1.1	Define Granular Control Access Rules & Policies Pt1	Network	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 identity, application, device, and traffic level 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	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	Enterprise and Component	Target Level ZT	8.3	The DoD Enterprise works with the 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 Segmentation 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&2).	SDN or alternative networking approach API's 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	Component	Target Level ZT	32.0	Following the API standards, requirements and SDN API functionalities, DoD Components will implement Software Defined 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 the 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	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 Segmentation. 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 moving laterally across the network.		B/C/P/S Macro segmentation; Application & Device Micro segmentation
5.3.1	Datacenter Macro segmentation	Network	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) 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
5.3.2	B/C/P/S Macro segmentation	Network	Component	Target Level ZT	18.1	DoD Components implement mission/organization-based macro-segmentation using logical network zones limiting 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) Component Principles (Asset Life cycle, Compliance, Policy). 2. Analyze Activities 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	

ID#	Activity Name	Pillar	Responsibility	Phase	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
5.4.1	Implement Micro segmentation	Network	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	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 functionalities – logical network zones, role, attribute and conditional based access control for user and devices, privileged access management services for network resources, and policy-based control on API access.	1. Assign Role, Attribute, & Condition Based Access Control to User & Devices. 2. Provide Privileged Access Management Services. 3. Limit Access on Per Identity Basis for User & Device. 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. Privileged access management 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
5.4.4	Protect Data In Transit	Network	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. DoD Provides Enterprise guidance 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. DiT 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 the Components to catalog and inventory existing Cyber Security policies and standards. Policies are updated and created in cross pillar activities as needed to meet critical ZT Target functionality.	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 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, 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 in organizations 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, and Device pillars. 2. Initial Enterprise profile rules for access standard is developed for access to DAAS. 3. When possible the Component profile(s) utilizes enterprise available services in the User, Data, Network 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	Phase	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	The Enterprise Security profile rules covers the User, Data, Network 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 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 least PDP(s), PEP(s), and PIP(s) details inventoried.	The patterns of behavior are established for what outcomes are needed for access control at the enterprise level.	Organization Access Profile	Enterprise Security Profile Pt2
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 possible 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 solution (SOAR) required to enable target level ZTA functionality where actionable and relevant information resides. DoD components identify instrument, integration, and interoperability points and prioritization-per the DoD enterprise baseline. The necessary integrations in User, Device, Application & Workload, Network and Device pillars to automate IR functions are completed.	1. DoD Enterprise establishes baseline integration and interoperability with SOAR to enable Target Level ZTA. 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 meeting key services and enabling recovery and protection capabilities.		Enterprise Integration & Workflow Provisioning Pt2
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 solution(s)/capability as needed. Machine Learning solution(s) is implemented in Components and existing tagged and classified data repositories are used to establish baselines. Machine learning solution(s) applies data tags in a supervised approach to continually improve analysis.	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 Pt~~1~~2
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.		
6.5.2	Implement SOAR Tools	Automation and Orchestration	Enterprise and Component	Target Level ZT	14.9	DoD Enterprise working with components to develop a standard set of requirements for security orchestration, automation, and response (SOAR) tooling to enable target level ZTA functions. 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 development Implementation Plan (e.g., Integration Points [Incident Response], Architecture, Interoperability, Scalability) 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	
6.6.1	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 compliant or non-compliant to Enterprise API standards.	Ensure tools includes a standardized API security with the proper protocols and capabilities to monitor, control access, and interoperate with other pillars.		

ID#	Activity Name	Pillar	Responsibility	Phase	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)

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 application programming interface (API) standard (or equivalent automated interchange mechanism) which at least outlines the approved patterns and protocols. DoD Components identify existing API's and update to the standard.	1. API Standard (or equivalent automated interchange mechanism) is established w/ 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 application/services (i.e., PEP, PDP, PIP) adopt the API standard. Information Systems required to follow ZT Target or Advanced should prioritized 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 Pt2.. 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 Component. 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
7.1.1	Scale Considerations	Visibility and Analytics	Component	Target Level ZT	11.6	DoD Components conduct analysis to determine current and future needs of scaling for monitoring, detection, and response. This requires a prioritization plan aligned with component business/mission considerations with associated risk alignment. Scaling is analyzed following common industry best practice methods and is in line 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 as components grow.	1. Evaluate opportunities for scaling (i.e., 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 also collaborating with BCP and DRP groups for distributed environment needs during emergencies and growth.		
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

ID#	Activity Name	Pillar	Responsibility	Phase	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
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 prioritized 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 (malware, phishing, etc.) Alerts and/or rule firings are fed into the parallel “Asset ID & Alert Correlation” activity to being 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
7.2.4	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 the accurate and detailed information. This information contributes to the incident response speed. Asset ID's also allow better visibility 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 to "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 off typical pattern and behavior in activity "Establish User Behavior Pattern" This approach will serve as a benchmark for security when identifying and responding to abnormal malicious activity.	1. Components Identify a subject/attribute baseline approach.	Components are able to utilize baseline approach to build profiles in activity Risk 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 provides intelligence and guidance to security teams in order to make improvements on threat monitoring and response.	Log Parsing	

ID#	Activity Name	Pillar	Responsibility	Phase	Duration	Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)
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 subject/attribute 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/Role Baseline 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 activity "Component Access Profile Rules" 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
7.5.1	Cyber Threat Intelligence Program Pt1	Visibility and Analytics	Enterprise and Component	Target Level ZT	9.9	The DoD Enterprise works with the 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 Cyber Threat Intelligence 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) (Build appropriate integration point 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 Intel is analyzed and appropriate actions and controls are enforced across ZT Pillars. Threat Intel Program adapts strategy over time with expansion of threat intel 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 data to support control enforcement to a greater extent throughout the organization via tooling.	Cyber Threat Intelligence Program Pt1	