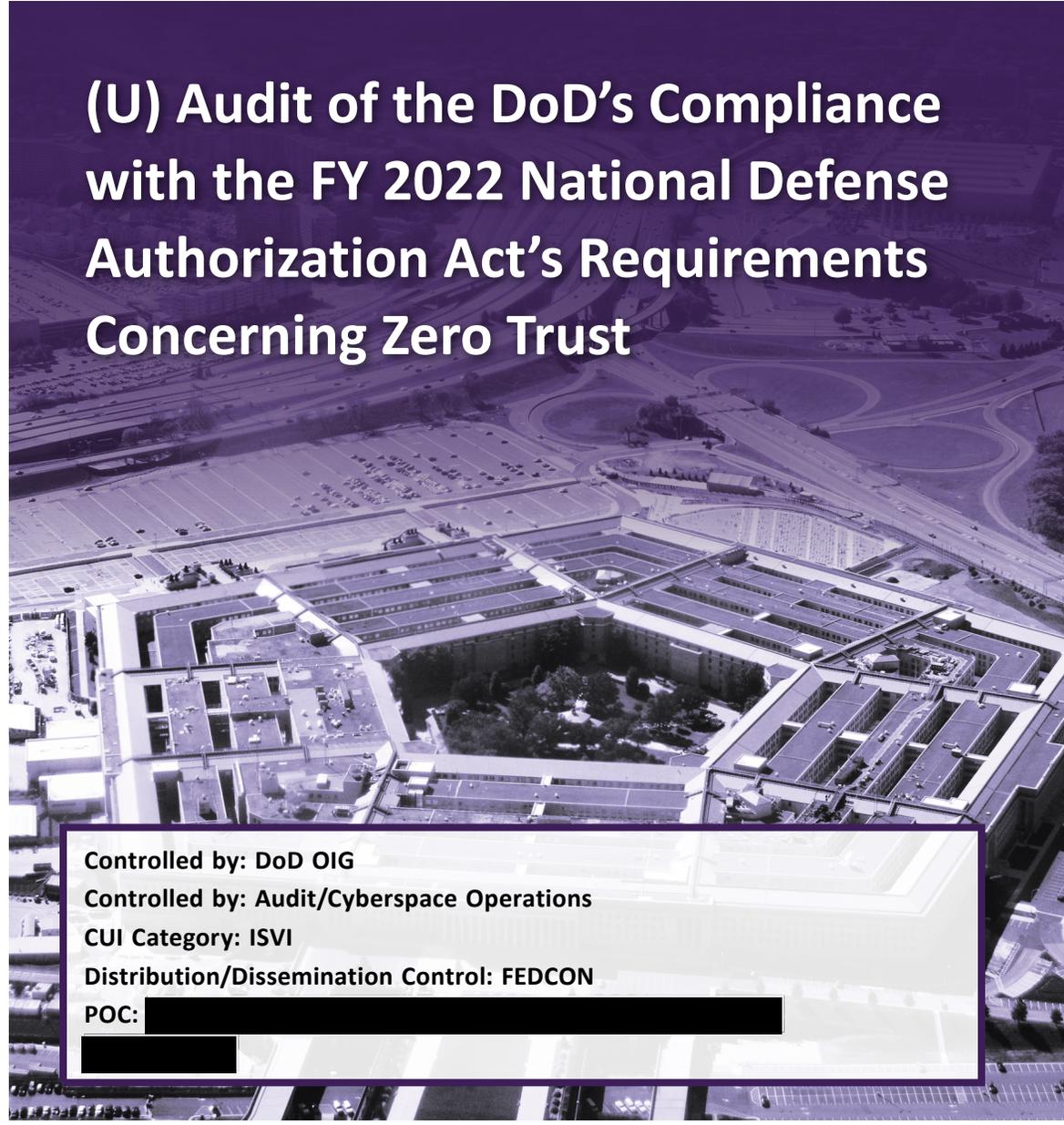


~~CUI~~

INSPECTOR GENERAL

U.S. Department of Defense

APRIL 29, 2025



(U) Audit of the DoD's Compliance with the FY 2022 National Defense Authorization Act's Requirements Concerning Zero Trust

Controlled by: DoD OIG
Controlled by: Audit/Cyberspace Operations
CUI Category: ISVI
Distribution/Dissemination Control: FEDCON
POC: [REDACTED]

INDEPENDENCE ★ INTEGRITY ★ EXCELLENCE ★ TRANSPARENCY

~~CUI~~





(U) Results in Brief

(U) Audit of the DoD's Compliance with the FY 2022 National Defense Authorization Act's Requirements Concerning Zero Trust

April 29, 2025

(U) Objective

(U) The objective of this audit was to determine whether the DoD complied with FY 2022 National Defense Authorization Act (NDAA) requirements to develop the DoD Zero Trust (ZT) strategy, principles, architecture, and implementation plans.

(U) Background

(U) ZT is a network cybersecurity model based on the premise that users and devices should never be automatically or implicitly trusted, whether operating inside or outside an organization's network perimeter. The FY 2022 NDAA directed the DoD Chief Information Officer (CIO) and the Commander, U.S. Cyber Command, to develop the DoD's ZT strategy, principles, and architecture across the DoD Information Network, including classified networks, operational technology, infrastructures, and weapon systems. The FY 2022 NDAA also required DoD Components to submit ZT implementation plans to the DoD CIO and the Commander of the Joint Forces Headquarters-Department of Defense Information Network no later than 1 year after the finalization of the ZT strategy.

(U) Findings

(U) The DoD generally complied with the FY 2022 NDAA requirements for ZT by developing its ZT strategy, principles, and reference architecture. However, the ZT Portfolio Management Office has not completed developing policies specific to operational technology, critical data,

(U) Findings (cont'd)

(U) infrastructures, and weapon systems, as required by the FY 2022 NDAA. The ZT Portfolio Management Office Director stated that once they complete research to identify viable ZT solutions for those environments, the policies will be developed.

~~(CUI)~~ In addition, of the 11 out of 45 DoD Component-level ZT implementation plans that we assessed, 7 of the plans included all the required elements, but the Defense Finance and Accounting Service, Defense Media Activity, National Guard Bureau, and Defense Legal Services Agency plans did not. Component officials provided different reasons for not including all of the elements, such as the need to identify all of their information technology assets before they could plan for ZT implementation.

[REDACTED]

(U) Although the DoD has taken the necessary action to meet most of the NDAA requirements for implementing ZT, it must continue to prioritize the establishment of the policies necessary to ensure that DoD Components implement ZT-based protections for operational technology, infrastructures, and weapon systems. Without those protections, there is greater risk that malicious cyber actors could access sensitive DoD information and adversely affect mission accomplishment and national security. Furthermore, the development of comprehensive ZT implementation plans for all DoD Components is critical to ensure that the DoD Components identify the acquisitions, funding, and policies needed for the effective implementation of ZT.

(U) Recommendations

(U) Among other recommendations, we recommend that the DoD CIO establish and implement a plan for accelerating the development of new policies and revision to existing policies specific to implementing the ZT framework on operational technology, infrastructures, and weapon systems, including



(U) Results in Brief

(U) Audit of the DoD's Compliance with the FY 2022 National Defense Authorization Act's Requirements Concerning Zero Trust

(U) Recommendations (cont'd)

(U) milestones for completion of those policies. We also recommend that the Defense Finance and Accounting Service, Defense Media Activity, National Guard Bureau, and Defense Legal Services Agency update and submit their Component-level ZT implementation plans to the DoD CIO.

(U) Management Comments and Our Response

(U) The Acting DoD CIO agreed with and provided their plan to address the recommendation for accelerating development of policies for implementing the ZT framework, therefore, the recommendation is closed. The Defense Finance and Accounting Service Director, Defense Media Activity Acting Director, Defense Legal Services Agency Director, and National Guard Bureau Chief

(U) agreed with and provided planned actions to address the recommendations to update and submit to the DoD CIO their Component-level ZT implementation plans; therefore, those recommendations are resolved. We will close the recommendations once we verify that management has taken the agreed upon actions.

(U) Although the National Guard Bureau Chief agreed with a recommendation to coordinate with the Army and Air Force concerning ZT capabilities, the planned actions did not meet the intent of the recommendation; therefore, the recommendation is unresolved. We request that the National Guard Bureau Chief provide additional comments within 30 days of the final report for the unresolved recommendation. Please see the Recommendations Table on the next page for the status of recommendations.

(U) Recommendations Table

| (U) Management | Recommendations Unresolved | Recommendations Resolved | Recommendations Closed |
|--|---------------------------------------|-------------------------------------|-----------------------------------|
| Chief, National Guard Bureau | B.3.a | B.3.b | None |
| Chief Information Officer of the Department of Defense | None | None | A.1 |
| Director, Defense Finance and Accounting Service | None | B.1 | None |
| Director, Defense Legal Services Agency | None | B.4 | None |
| Director, Defense Media Activity | None | B.2.a, B.2.b | None (U) |

(U) Please provide Management Comments by May 29, 2025.

(U) Note: The following categories are used to describe agency management’s comments to individual recommendations.

- **(U) Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **(U) Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **(U) Closed** – The DoD OIG verified that the agreed upon corrective actions were implemented.





OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

April 29, 2025

MEMORANDUM FOR CHIEF, NATIONAL GUARD BUREAU
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE
DIRECTOR, DEFENSE LEGAL SERVICES AGENCY
DIRECTOR, DEFENSE MEDIA ACTIVITY

SUBJECT: (U) Audit of the DoD's Compliance with the FY 2022 National Defense Authorization Act's Requirements Concerning Zero Trust (Report No. DODIG-2025-090)

(U) This final report provides the results of the DoD Office of Inspector General's audit. We previously provided copies of the draft report and requested written comments on the recommendations. We considered management's comments on the draft report when preparing the final report. These comments are included in the report.

(U) This report contains one recommendation that we consider unresolved because the National Guard Bureau Chief did not fully address the recommendation. We will track the recommendation until the National Guard Bureau Chief has agreed to take actions that we determine to be sufficient to meet the intent of the recommendation and provides documentation showing that all agreed-upon actions to implement the recommendation are completed.

(U) This report contains five recommendations that we consider resolved but open. We will close the recommendations when the Defense Finance and Accounting Service Director, Defense Media Activity Acting Director, and Defense Legal Services Agency Director provide documentation showing that all agreed-upon actions to implement the recommendations are completed.

(U) This report contains one recommendation that we consider closed because the DoD Chief Information Officer took action to fully address the recommendation.

(U) DoD Instruction 7650.03 requires that recommendations be resolved promptly. For the unresolved recommendation, please provide us within 30 days your response concerning specific actions in process or alternative corrective actions proposed on the recommendation. For the resolved but open recommendations, please provide us within 90 days documentation showing that the agreed-upon actions have been completed. Send your responses to either [REDACTED] if unclassified or [REDACTED] if classified SECRET.

(U) We appreciate the cooperation and assistance received during the audit. If you have any questions, please contact me at [REDACTED].

A handwritten signature in cursive script that reads "Carol N. Gorman".

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

(U) Contents

(U) Introduction

| | |
|----------------------|---|
| (U) Objective | 1 |
| (U) Background | 1 |

(U) Finding A. The DoD Developed Its ZT Strategy, Principles, and Architecture but Did Not Fully Comply with FY 2022 NDAA Requirements for Developing ZT Policies

6

| | |
|--|----|
| (U) The DoD Generally Complied with the FY 2022 NDAA’s Requirements for Zero Trust | 6 |
| (U) The ZT PfMO Had Not Completed Policies for Implementing Zero Trust for Operational Technology, Infrastructures, and Weapon Systems | 11 |
| (U) The DoD Needs to Ensure Compliance with All NDAA ZT Requirements | 12 |
| (U) Recommendation, Management Comments, and Our Response | 12 |

(U) Finding B. DoD Components Did Not Always Submit ZT Implementation Plans that Included the Required FY 2022 NDAA Elements

14

| | |
|---|----|
| (U) DFAS, the DMA, and the NGB Did Not Include Required Elements in Their ZT Implementation Plans, and the DLSA Did Not Submit a Plan | 15 |
| (U) Ensuring that ZT Implementation Plans Contain the Correct Information Is Critical | 18 |
| (U) Management Comments on the Report and Our Response | 18 |
| (U) Recommendations, Management Comments, and Our Response | 20 |

(U) Appendixes

| | |
|--|----|
| (U) Appendix A. Scope and Methodology | 24 |
| (U) Internal Control Assessment and Compliance | 25 |
| (U) Use of Computer-Processed Data | 25 |
| (U) Use of Technical Assistance | 25 |
| (U) Prior Coverage | 25 |
| (U) Appendix B. FY 2022 National Defense Authorization Act Zero Trust Requirements | 26 |
| (U) Appendix C. DoD Zero Trust Component Implementation Plan Template | 30 |

(U) Contents (cont'd)

(U) Management Comments

| | |
|---|----|
| (U) National Guard Bureau..... | 32 |
| (U) DoD Chief Information Officer..... | 34 |
| (U) Defense Finance and Accounting Service..... | 35 |
| (U) Defense Information Systems Agency..... | 36 |
| (U) Defense Legal Services Agency..... | 40 |
| (U) Defense Media Activity..... | 41 |

(U) Acronyms and Abbreviations..... 42



(U) Introduction

(U) Objective

(U) The objective of this audit was to determine whether the DoD complied with requirements to develop its Zero Trust (ZT) strategy, principles, architecture, and implementation plans in accordance with the FY 2022 National Defense Authorization Act (NDAA). The scope, methodology, and prior coverage related to the objective are in Appendix A.¹

(U) Background

(U) ZT is a network cybersecurity model based on the premise that users and devices should never be automatically or implicitly trusted whether operating inside or outside an organization's network perimeter. By default, ZT assumes that every access request, regardless of its origin or location, should be strictly and continually verified and authenticated before access to a network is granted or maintained. ZT is designed to prevent data breaches and limit lateral movement within a network once initial network access is granted. The basic assumptions supporting ZT include the following elements.

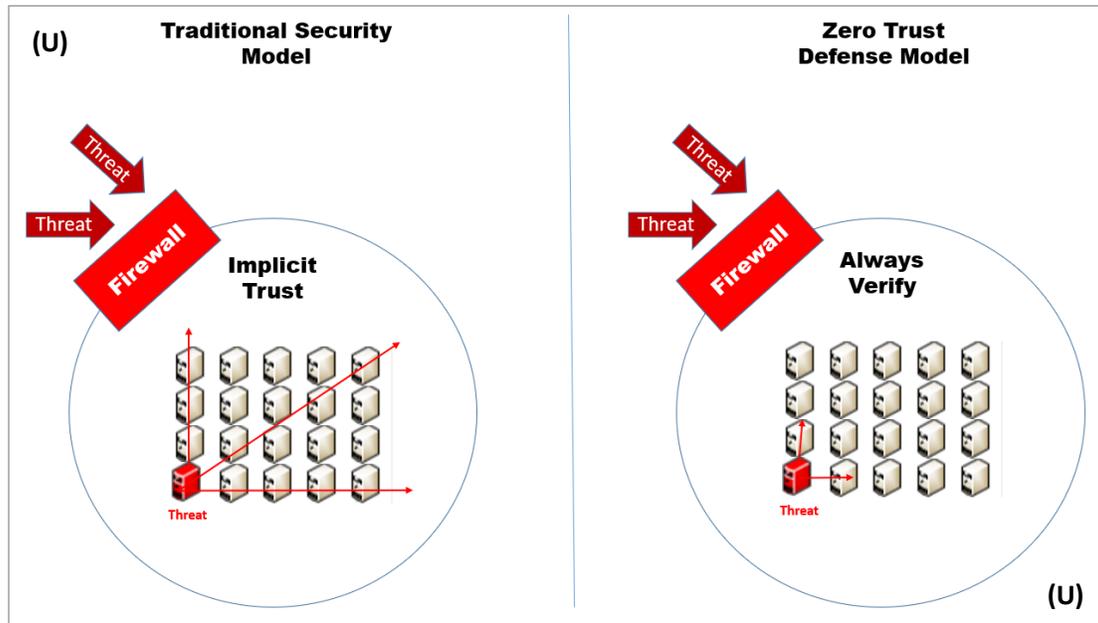
- **(U) Assume a Hostile Environment.** There are malicious cyber actors both inside and outside a network environment. Therefore, all users, devices, applications, and environments are treated as untrusted.
- **(U) Presume a Breach.** There are hundreds of thousands of attempted cybersecurity attacks every day. Therefore, organizations need to consciously operate and defend resources with the assumption that an adversary has presence within their environment.
- **(U) Never Trust, Always Verify.** All devices, users, applications, and data flows should not be trusted and should always be authenticated and explicitly authorized.²
- **(U) Scrutinize Explicitly.** All resources are consistently accessed in a secure manner. Access to resources is conditional and can change based on analyzing user behaviors to detect abnormal and malicious cyber activities.
- **(U) Apply Analytics.** Apply analytics to data, applications, assets, services including behavior metrics, and log each transaction.

¹ (U) This report contains information that has been redacted because it was identified by the Department of Defense as Controlled Unclassified Information (CUI) that is not releasable to the public. CUI is Government-created or owned unclassified information that allows for, or requires, safeguarding and dissemination controls in accordance with laws, regulations, or Government-wide policies.

² (U) Data flow is the movement of data through a system composed of software, hardware, or a combination of both.

(U) ZT differs from more traditional information technology (IT) security models in which users and devices are trusted once given access to the network, allowing them the ability to move laterally through the network without additional authentication or verification. Figure 1 depicts the difference between a traditional security model and a ZT defense model. The traditional security model and ZT defense model both require initial authentication and verification before a user can access a network, but the ZT defense model also employs “continuous verification” each time a user attempts to move across the network. If a malicious cyber actor was able to bypass the network firewall and gain initial authentication and verification, the ZT defense model would limit their ability to move beyond the initial point of entry and access other parts of the network without additional authentication and verification.

(U) Figure 1. Traditional Security Model and Zero Trust Defense Model



(U) Source: The DoD OIG.

(U) FY 2022 NDAA Zero Trust Requirements

(U) The FY 2022 NDAA directed the DoD Chief Information Officer (CIO) and the Commander, U.S. Cyber Command, to jointly develop the DoD's ZT strategy, principles, and architecture no later than 270 days after the enactment of the FY 2022 NDAA.³ The FY 2022 NDAA required that the DoD's ZT strategy, principles, and architecture include the following elements.⁴

- (U) Prioritized policies and procedures for establishing the implementation of ZT-enabling capabilities and access control policies related to, among other things, access management; encryption; data loss detection and prevention; and configuration management⁵
- (U) Policies specific to operational technology, critical data, infrastructures, weapon systems, and classified networks
- (U) Specifications for enterprise-wide acquisitions of capabilities in support of ZT for operational technology, critical data, infrastructures, weapon systems, and classified networks
- (U) Specifications for standard ZT principles that support reference architectures and metrics-based assessment plans⁶
- (U) Roles, responsibilities, functions, and operational workflows for the ZT cybersecurity architecture and IT personnel

(U) Operational technology is hardware and software needed to run daily operations. Critical data is information considered essential to execute an organization's mission. Infrastructures are basic physical structures needed for the operation of an enterprise. A weapon system is a combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment. A classified network stores sensitive information and requires access controls to be in place to ensure that information is not accessible to the public.

³ (U) Public Law 117-81, "National Defense Authorization Act for Fiscal Year 2022," section 1528, "Zero trust strategy, principles, model architecture, and implementation plans," December 27, 2021. Section 1528 is included in its entirety in Appendix B. The FY 2022 NDAA was enacted on December 27, 2021; therefore, the DoD was required to develop the documents no later than September 27, 2022.

⁴ (U) A ZT architecture refers to how software and hardware connect and interact within a network in a ZT environment.

⁵ (U) According to the FY 2022 NDAA, the policies and procedures should include, among other requirements, identity, credential, and access management controls; network segmentation; data management, data rights management, and access controls; encryption; user access and behavioral monitoring, logging, and analysis; data loss detection and prevention methodologies; and least privilege, including system or network administrator privileges.

⁶ (U) A reference architecture establishes a framework that includes conceptual descriptions of an architecture and its capabilities. The metrics-based assessment plans should be designed to provide the data needed to determine whether implementation of the DoD ZT Strategy delivers the expected benefits.

(U) The FY 2022 NDAA also required the DoD Components to submit ZT implementation plans to the DoD CIO and the Commander of the Joint Forces Headquarters-Department of Defense Information Network no later than 1 year after the finalization of the ZT strategy.⁷ At a minimum, the FY 2022 NDAA required that the ZT implementation plans include the following elements.

- (U) Specific acquisitions, implementations, instrumentations, and operational workflows to be implemented across unclassified and classified networks, operational technology, and weapon systems⁸
- (U) A detailed schedule with targeted milestones and required expenditures
- (U) Interim and final metrics, including a phased migration plan
- (U) Identification of additional funding, authorities, and policies, as necessary
- (U) Requested waivers, exceptions to DoD policy, and expected delays

(U) DoD Zero Trust Portfolio Management Office

(U) In January 2022, the DoD CIO established the DoD ZT Portfolio Management Office (ZT PfMO) to coordinate the DoD's efforts to accelerate ZT adoption. The ZT PfMO is responsible for aligning the ZT efforts of DoD Components by providing guidance and identifying and advocating for the resources needed to implement ZT and synchronize DoD ZT adoption.⁹ In addition, the ZT PfMO is responsible for coordinating with DoD Components to define, develop, and adapt their respective ZT implementation plans to comply with the FY 2022 NDAA. In August 2023, the ZT PfMO developed the first DoD ZT Component Implementation Plan Template. See Appendix C for a table that identifies how the FY 2024 Implementation Plan Template aligns with the required FY 2022 NDAA elements.

(U) The Defense Information Systems Agency's Thunderdome

(U) In support of the DoD's ZT implementation, the Defense Information Systems Agency (DISA) is developing an enterprise ZT solution, known as Thunderdome, that is intended to be available to DoD Components to secure access to applications and data; protect enclaves; and protect applications operating in a cloud

⁷ (U) The "DoD Zero Trust Strategy" was released on October 21, 2022, resulting in a deadline of October 21, 2023, for DoD Components to submit their ZT implementation plans.

⁸ (U) Instrumentations involve analyzing information flow across the infrastructure.

⁹ (U) According to the ZT PfMO Director, the DoD CIO is responsible for implementing ZT on the Non-classified Internet Protocol Router Network and SECRET Internet Protocol Router Network, and all policies and procedures developed by the ZT PfMO apply to both of those networks. The Office of the Director of National Intelligence is responsible for implementing ZT on the Joint Worldwide Intelligence Communications System and special access networks. The Joint Worldwide Intelligence Communications System is the network that houses information up to the Top Secret and Secure Compartmented Information levels. Special access networks house classified information in Special Access Programs.

(U) environment or on-premises.¹⁰ According to DISA, Thunderdome will include a suite of IT and cyber-based technologies that will leverage enterprise identity and access management to achieve ZT. Thunderdome is expected to include network and security tools designed to provide the protection and reliability of DoD networks. DISA expects Thunderdome to be fully operational by FY 2027.

(U) DoD Components Assessed

(U) To determine whether the DoD complied with the FY 2022 NDAA requirements to develop its ZT strategy, principles, architecture, and implementation plans, we reviewed the DoD ZT Strategy and ZT Reference Architecture (ZTRA)—both of which included the ZT principles for achieving ZT—to determine whether they aligned with the requirements.¹¹ We also selected 11 out of 45 Component-level ZT implementation plans to review. Two of the 11 plans incorporated plans from four other DoD Components; therefore, our review covered 15 DoD Components, as identified in Table 1. We reviewed each of the DoD Component ZT implementation plans to determine whether they included the elements required by the FY 2022 NDAA.

(U) Table 1. DoD Components Selected for Implementation Plan Review

| (U) DoD Components |
|--|
| U.S. Army |
| U.S. Navy (applies to the U.S. Marine Corps and U.S. Indo-Pacific Command) |
| U.S. Air Force (applies to the U.S. Space Command and U.S. Space Force) |
| National Guard Bureau (NGB) |
| Defense Finance and Accounting Service (DFAS) |
| Defense Health Agency |
| Defense Information Systems Agency (DISA) |
| Defense Legal Services Agency (DLSA) |
| Defense Threat Reduction Agency |
| Defense Media Activity (DMA) |
| Office of Local Defense Community Cooperation (U) |

(U) Source: The DoD OIG.

¹⁰ (U) Enclaves are a set of system resources that operate in the same security domain and share the protection of a single, common, continuous security perimeter. On-premises refers to a computing model in which an organization manages and hosts its own hardware, software applications, and data within its physical location, such as in an office building or a dedicated data center. The organization is responsible for purchasing, installing, configuring, maintaining, and securing all the components of its IT infrastructure.

¹¹ (U) The DoD refers to its ZT architecture as the ZT Reference Architecture.

(U) Finding A

(U) The DoD Developed Its ZT Strategy, Principles, and Architecture but Did Not Fully Comply with FY 2022 NDAA Requirements for Developing ZT Policies

(U) The DoD generally complied with the FY 2022 NDAA requirements for ZT by developing the DoD ZT Strategy, ZT principles, and ZTRA. However, the ZT PfMO has not completed developing policies specific to: (1) operational technology, (2) critical data, (3) infrastructures, and (4) weapon systems, as required by the FY 2022 NDAA. The ZT PfMO Director stated that they are conducting research to identify and test potential ZT solutions for those non-information technology environments because constraints, such as different and incompatible approaches for implementing ZT on IT environments and operational technology, make it difficult to implement ZT in the same manner as it is implemented for the DoD's Non-classified Internet Protocol Router Network and SECRET Internet Protocol Router Network. The ZT PfMO Director also stated that once viable solutions are identified, the ZT policies will be developed. We acknowledge that operational technology, infrastructure, and weapons systems within the DoD are complex and have unique security challenges, and identifying and testing ZT solutions for these areas is taking additional time; however, the DoD must continue to prioritize the development, integration, and deployment of effective ZT solutions to secure critical systems and data across all operational environments. Operational technology, infrastructure, and weapon systems provide significant attack surface opportunities for malicious cyber actors to access sensitive DoD information and systems through supply chain vulnerabilities and unpatched or legacy systems. Those vulnerabilities can provide a greater level of risk and exposure which could adversely affect mission accomplishment and impact national security.

(U) The DoD Generally Complied with the FY 2022 NDAA's Requirements for Zero Trust

(U) The DoD generally complied with the FY 2022 NDAA's requirements for ZT by developing the DoD ZT Strategy, ZT principles, and ZTRA. In those documents, the DoD established policies on access controls, specifications for acquisition and ZT principles, and roles and responsibilities for ZTRA and IT personnel.

(U) Zero Trust Strategy, Principles, and Architecture

(U) In July 2022, the DoD issued the “Department of Defense Zero Trust Reference Architecture,” Version 2.0, which met the FY 2022 NDAA requirement to develop a ZT architecture within 270 days of enactment of the FY 2022 NDAA.¹² The ZTRA establishes the DoD’s ZT framework, identifies strategic goals and objectives for ZT, and supports IT investment decisions. The ZTRA identifies specific capabilities for implementing ZT and includes 17 examples that Components can use to customize ZT solutions to meet their organizational needs based on requirements, structures, and security policies. The examples include diagrams and flowcharts that highlight the differences between traditional and ZT network environments.

(U) On October 21, 2022, the DoD issued the “DoD Zero Trust Strategy” that defines how the DoD plans to accelerate the shift to a ZT architecture framework. The DoD ZT Strategy incorporates the following DoD ZT principles required by the FY 2022 NDAA, which are designed to support the development and revision of strategy, policy, design, and execution documents for ZT.¹³

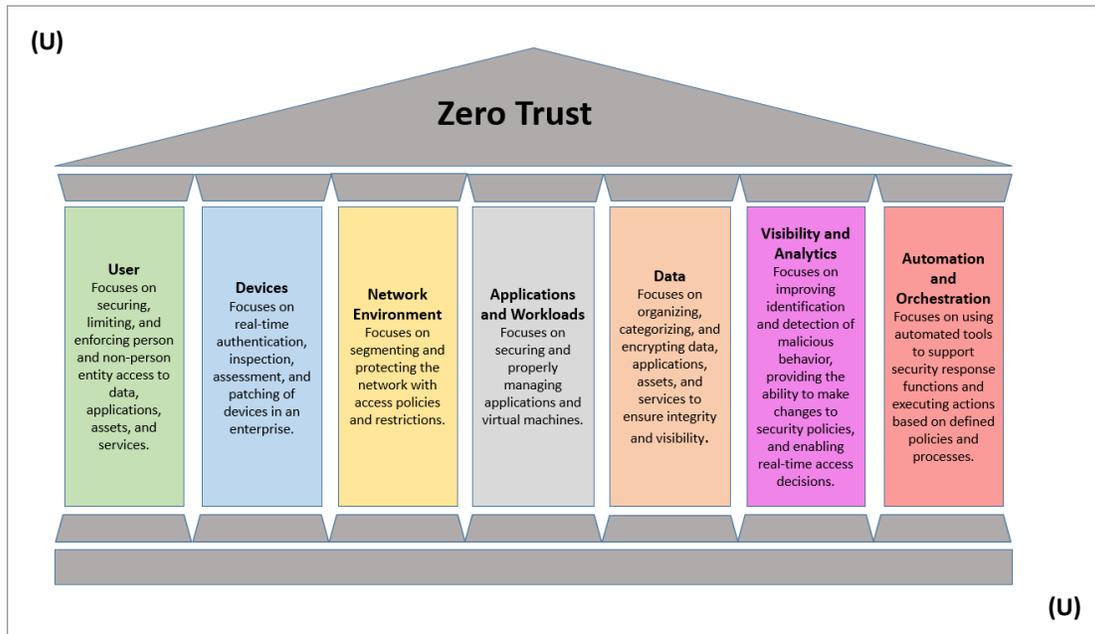
- **(U) Mission-Oriented.** Ensure that all users and non-person entities can access, collaborate, work, and execute missions on any network for which they both have the need and right to access.¹⁴
- **(U) Organizational.** Limit the extent and reach of potential damage incurred by a breach by restricting access, reducing the attack surface, and monitoring risks in real-time.
- **(U) Governance.** Establish appropriate governance controls that continuously modernize the existing fragmented approaches to data management, IT modernization, and cybersecurity policies and solutions.
- **(U) Technical.** Align technical and security programs with ZT goals and mission objectives to streamline regulations and standards for managing security and risk.

(U) To accomplish the ZT principles, the DoD ZT Strategy includes seven ZT pillars and the associated capabilities and activities that outline a standardized methodology for executing ZT across the DoD. Figure 2 describes the seven DoD ZT pillars.

¹² (U) The first version of the ZTRA was published on May 13, 2021.

¹³ (U) Although the DoD ZT Strategy was not issued within the required 270 days, we did not consider this a material deficiency because the strategy was issued within 30 days of the requirement.

¹⁴ (U) Non-person entities include organizations, hardware devices, and software applications.

(U) Figure 2. DoD Zero Trust Pillars

(U) Source: The DoD OIG.

(U) The DoD ZT Strategy requires that the DoD Components reach a target level for each ZT capability by the end of FY 2027. The target-level ZT is a set of minimum requirements that the DoD Components must achieve for successful ZT implementation.

(U) NDAA-Required Elements Addressed in the DoD's ZT Strategy, Principles, and Architecture

(U) The DoD addressed the NDAA-required elements in the DoD ZT Strategy, ZT principles, and ZTRA, including policies on access controls, specifications for acquisition and ZT principles, and roles and responsibilities for the ZTRA and IT personnel. Table 2 provides the DoD actions taken related to the required elements.

(U) Table 2. Actions Taken to Meet the NDAA-Required Elements

| (U) FY 2022 NDAA-Required Element | Action Taken by the DoD |
|--|---|
| <p>Prioritized policies and procedures for implementing ZT-enabling capabilities and access control policies related to, among other things, access management; encryption; data loss detection and prevention; and configuration management</p> | <p>The ZT Strategy includes lists of the DoD’s existing policies and procedures that addressed, or needed to be revised to adequately address, implementation of ZT-enabled capabilities.</p> <p>The ZT PfMO listed the following as prioritized policies for implementing ZT.</p> <ul style="list-style-type: none"> • Data Tagging Standards • Access Control • Data Rights Management • Comply-to-Connect • Public Key Infrastructure <p>The ZT PfMO plans to catalog all of the DoD’s information technology policies that require ZT-related procedures. The target completion dates for the policies and procedures range from September 30, 2025, to December 31, 2025.</p> <p>Some of the DoD’s existing policies also include requirements related to ZT. For example:</p> <ul style="list-style-type: none"> • DoD Instruction 8520.04, "Access Management for DoD Information Systems," September 3, 2024, requires that system access be granted based on the principle of least privilege and requires information owners to implement the Identity Credential and Access Management principles.¹ • DoD Instruction 8520.03, "Identity Authentication for Information Systems," May 19, 2023, requires multifactor authentication.² <p>While all of the DoD’s policies have not been revised to include ZT protections, the ZT PfMO reviewed the following policies and submitted comments to incorporate ZT.</p> <ul style="list-style-type: none"> • Draft Committee on National Security System Policy No. 21, “National Cybersecurity Policy on Zero Trust for National Security Systems” • DoD Instruction 8580.01, “Cybersecurity in Defense Acquisition” • DoD Directive 8500.03, “DoD Cybersecurity Program” |
| <p>Specifications for enterprise-wide acquisitions of capabilities conducted or to be conducted regarding the policies for operational technology, critical data, infrastructures, weapon systems, and classified networks</p> | <p>The ZTRA includes specifications for enterprise-wide acquisitions of ZT capabilities in support of ZT for operational technology, critical data, infrastructures, weapon systems, and classified networks. Subsequent to the issuance of the ZTRA, DISA is developing Thunderdome, an enterprise-wide ZT solution for all DoD Components that are on the DoD Network.³ As of January 2025, Thunderdome covered 85 of the 91 activities required to achieve target-level ZT. DoD Components that have systems that are not on the DoD Network are responsible for identifying and implementing a ZT solution of their choice but have the option to purchase Thunderdome services from DISA.</p> |

(U)

(U) Table 2. Actions Taken to Meet the NDAA-Required Elements (cont'd)

| (U) FY 2022 NDAA-Required Element | Action Taken by the DoD |
|---|--|
| Specifications for standard ZT principles that support reference architectures and metrics-based assessment plans | <p>The ZTRA includes the specifications for the following ZT guiding principles that support the reference architecture, in the form of 17 examples that Components can use to customize their ZT solutions.</p> <ul style="list-style-type: none"> • Assume no implicit or explicit trusted zone in networks. • Strictly enforce identity-based authentication and authorization for all connections and access to infrastructure, data, and services. • Strictly enforce authentication and authorization for communication between servers and the applications. • Use risk profiles that are generated from monitoring user and device behaviors to authorize users and devices to resources. • Encrypt sensitive data in transit and data at rest.⁴ • Continuously monitor, collect, store, and analyze all events and assess compliance with security policies. • Centralize policy management and distribution. <p>In addition, the DoD CIO directed the DoD Components to include in their implementation plans ZT Strategy metrics for measuring compliance with deadlines for completing ZT activities; ZT planning; development of a ZT culture by conducting ZT education and training; and assessment of ZT activity outcomes. As discussed in Finding B of this report, most of the DoD Components that we reviewed included this information in their implementation plans.</p> |
| Roles, responsibilities, functions, and operational workflows for ZT cybersecurity architecture and IT personnel | <p>The DoD ZT Strategy includes roles and responsibilities for the DoD PfMO, system owners, and DoD Components with respect to the ZT architecture. To formalize the roles and responsibilities, in August 2024, the DoD CIO distributed a draft directive-type memorandum for comments related to implementing the DoD ZT Strategy. The draft memorandum lists the roles and describes the responsibilities for the DoD CIO, the Under Secretary of Defense for Acquisition and Sustainment, and DISA Director, who are responsible for overseeing and implementing ZT. For example, the DoD CIO is responsible for overseeing the implementation of the DoD ZT Strategy; the Under Secretary of Defense for Acquisition and Sustainment is responsible for incorporating ZT strategic principles into critical infrastructures and weapon systems; and the DISA Director is responsible for aligning enterprise services to address the adoption of ZT. The draft memorandum also states that DoD Component Heads should identify, in their ZT implementation plans, which personnel require specialized ZT training.</p> <p style="text-align: right;">(U)</p> |

¹ (U) Identity Credential and Access Management principles are programs, processes, and technologies that are used to create trusted digital identities of individuals and entities and assigns those identities to credentials to provide authorized access to an agency's resources.

² (U) Multifactor authentication is a process that requires using two or more factors to achieve authentication. Factors include something you know, something you have, or something you are.

³ (U) The DoD Network consolidates the DoD Agencies and Field Activities into a single operating environment. DoD Agencies and Field Activities are agencies that provide support services to the DoD, such as accounting, payroll, logistics, and supply services. The DoD Agencies and Field Activities began migrating to the DoD Network in FY 2024.

⁴ (U) Data in transit is data that moves from one point to another, such as data moving through an email. Data at rest is data that is stored and not actively being accessed, such as stored files on a server or hard drive.

(U) Source: The DoD OIG.

(U) The ZT PfMO Had Not Completed Policies for Implementing Zero Trust for Operational Technology, Infrastructures, and Weapon Systems

(U) As of November 2024, the ZT PfMO had not completed developing policies specific to operational technology, critical data, infrastructures, and weapon systems, as required by the FY 2022 NDAA. The ZT PfMO Director stated that constraints exist for implementing ZT in those environments because they have unique mission and system parameters that limit the ZT capabilities that can be applied. For example, applying ZT principles, such as real-time continuous authentication to weapon systems, requires continuous verification of system processes. That continuous verification could delay the timing of weapon operations, such as munition deployment, and result in mission failure.

(U) The ZT PfMO has taken steps towards understanding how to apply ZT to operational technology, infrastructures, and weapon systems by establishing working groups to identify strategies and approaches for applying ZT in operational technology, infrastructures, and weapon systems. The working groups include representatives from the Under Secretary of Defense for Acquisition and Sustainment and DoD Components, such as the Under Secretary of Defense for Acquisition and Sustainment's Cyber Warfare Directorate, Joint Forces Headquarters – Department of Defense Information Network, and industry partners. According to the ZT PfMO, the working groups are responsible for developing best practices and ZT activity baselines for ZT implementation on operational technology, infrastructures, and weapon systems, and the ZT PfMO will use the information gathered during the working groups to develop policies, architectures, and requirements for these environments.

(U) In addition, the ZT PfMO Director stated that the actions taken by the ZT PfMO toward achieving target-level ZT stimulated industry partners to invest and innovate ZT solutions that fit DoD requirements. However, the Director stated that, until the ZT PfMO determines an outcomes-based approach for implementing ZT on information technology that is proven and sustainable, it would be challenging to develop ZT solutions for three different technologies simultaneously while trying to define ZT itself.

(U) We acknowledge that operational technology, infrastructure, and weapons systems within the DoD are complex and have unique security challenges, and identifying and testing ZT solutions for these areas takes additional time. However, the DoD needs to prioritize the development, integration, and deployment of effective ZT solutions to secure critical systems and data across all operational environments and track the progress of those solutions and development of the corresponding policy.

(U) The DoD Needs to Ensure Compliance with All NDAA ZT Requirements

(U) Although the DoD has taken the necessary action to meet most of the NDAA requirements for implementing ZT, it must prioritize the establishment of the policies necessary to ensure that DoD Components implement ZT-based protections for operational technology, infrastructures, and weapon systems. ZT-based protections for operational technology, infrastructures, and weapon systems reduce the risk that malicious cyber actors infiltrate critical areas that are vital to the health and safety of U.S. citizens. Examples of critical areas that require ZT-based protections are as follows.

- (U) Heating, ventilation, and air conditioning systems (operational technology) ensure the sterility in operating rooms at military hospitals.
- (U) U.S. drinking water treatment facilities (critical infrastructure) ensure U.S. military personnel and civilians have clean water for everyday use.
- (U) Weapon systems ensure that the DoD can counter adversarial attacks without delays.

(U) Operational technology, infrastructure, and weapon systems provide significant attack surface opportunities for malicious cyber actors to access sensitive DoD information and systems through supply chain vulnerabilities and unpatched or legacy systems. Those vulnerabilities can provide a greater level of risk and exposure which could adversely affect mission accomplishment and impact national security.

(U) Recommendation, Management Comments, and Our Response

(U) Recommendation A.1

(U) We recommend that the DoD Chief Information Officer establish and implement a plan for accelerating the development of new policies and revision to existing policies specific to implementing the Zero Trust framework on operational technology, infrastructures, and weapon systems, including milestones for completion of those policies.

(U) DoD Chief Information Officer Comments

(U) The Acting DoD CIO agreed, stating that the ZT PfMO created and implemented a ZT Policy Playbook with a Plan of Action and Milestones that will accelerate policy issuance and that included milestones for developing new and revising existing policies. The Acting DoD CIO also stated that in accordance with the Playbook, they will establish ZT policies and guidance for operational technology by December 2025, and work with the Under Secretary of Defense for Acquisition and Sustainment, the Joint Chiefs of Staff, and the Military Services to establish policies for infrastructure and weapon systems by December 2026.

(U) Our Response

(U) Comments from the Acting DoD CIO addressed all specifics of the recommendation. We reviewed the ZT Policy Playbook and Plan of Action and Milestones and verified that it included actions and milestones to accelerate policy issuance specific to the ZT framework; therefore, the recommendation is closed.

(U) Finding B

(U) DoD Components Did Not Always Submit ZT Implementation Plans that Included the Required FY 2022 NDAA Elements

(U) DoD Components did not always submit ZT implementation plans that included all of the elements required by the FY 2022 NDAA. Of the 11 out of 45 DoD Component-level implementation plans that we assessed, 7 of the plans included all the required elements and were submitted in a timely manner. Although DFAS, the DMA, and the NGB submitted ZT implementation plans, the plans did not include all the required elements. In addition, the NGB plan was not submitted timely and the DLSA did not submit a plan.

- ~~(CUI)~~ The DFAS ZT implementation plan did not include information about [REDACTED]. The DFAS Director for ZT Architecture stated that DFAS was waiting for DISA to determine the ZT capabilities that Thunderdome would offer to understand which capabilities DFAS needed for their networks. The DFAS Director for ZT Architecture also stated that [REDACTED].
- (U) The DMA ZT implementation plan did not include information about specific acquisitions, implementations, instrumentations, and operational workflows; a detailed schedule with target milestones; interim and final metrics, including a phased migration plan; or the identification of additional funding, authorities, and policies. The DMA CIO stated that the information was not included because the DMA did not have full visibility of DMA IT assets, and that although the DMA was working with DISA to identify DMA IT assets, that effort was not yet complete.
- (U) The NGB ZT implementation plan was submitted on February 5, 2024, 107 days after the October 21, 2023 due date. When submitted, the NGB ZT implementation plan did not include information about specific acquisitions, implementations, instrumentations, and operational workflows; a detailed schedule with target milestones; interim and final metrics, including a phased migration plan; or the identification of additional funding, authorities, and policies. The NGB Chief of Strategy and Governance stated that the information was not provided because

(U) the NGB officials believed the Army and Air Force’s implementation plan would include NGB systems since the systems reside on the Army and Air Force networks.

- (U) The DLSA did not submit a ZT implementation plan. The DLSA IT Chief stated that they did not submit a plan because they needed information from DISA since DISA hosts the DLSA’s mission-specific systems.

(U) Submission of incomplete DoD Component ZT implementation plans limits the DoD’s ability to address gaps in acquisition, funding, and policy to meet the ZT requirements in the FY 2022 NDAA and to track each DoD Component’s progress toward meeting the FY 2027 deadline for ZT implementation.

(U) DFAS, the DMA, and the NGB Did Not Include Required Elements in Their ZT Implementation Plans, and the DLSA Did Not Submit a Plan

(U) Of the 11 DoD Component-level implementation plans that we assessed, 7 of the plans included all of the required elements and were submitted in a timely manner. Although DFAS, the DMA, and the NGB submitted ZT implementation plans, the plans did not include all of the required elements. In addition, the NGB plan was not submitted in a timely manner, and the DLSA did not submit a plan. Table 3 identifies the FY 2022 NDAA elements that were not addressed.

(U) Table 3. NDAA Elements Not Addressed by DFAS, the DMA, NGB, and DLSA

| (CUI) FY 2022 NDAA Elements for Developing Component-Level Implementation Plans | DoD Component | | | |
|---|---------------|-----|-----|------|
| | DFAS | DMA | NGB | DLSA |
| Specific acquisitions, implementations, instrumentations, and operational workflows to be implemented across unclassified and classified networks; operational technology; and weapon systems | █ | X | X | X |
| Detailed schedule with target milestones and required expenditures | █ | X | X | X |
| Interim and final metrics, including a phased migration plan | █ | X | X | X |
| Identification of additional funding, authorities, and policies, as necessary | █ | X | X | X |
| Requested waivers, exceptions to DoD policy, and expected delays | █ | ✓ | X | X |

~~(CUI)~~

(U) Source: The DoD OIG.

~~(CUI)~~ ***The Defense Finance Accounting Service ZT Implementation Plan Did Not Include [REDACTED]***

~~(CUI)~~ The DFAS Director for ZT did not include all the FY 2022 NDAA elements in the DFAS ZT implementation plan. Specifically, the plan did not include information about [REDACTED]

[REDACTED]. In addition, the plan did not include [REDACTED]

~~(CUI)~~ According to the DFAS Director for ZT Architecture, since DFAS heavily relies on DISA to provide services for network connections, telecommunications, database administration, and cybersecurity defense, DFAS was waiting for DISA to determine the ZT capabilities that Thunderdome would offer to understand which capabilities DFAS needed for their networks.¹⁵ The DFAS Director for ZT Architecture stated that without this understanding, [REDACTED]

However, as of October 2024, DISA had developed a list of ZT capabilities that Thunderdome offers, which should allow DFAS to update their ZT implementation plan accordingly. The DFAS Director for ZT Architecture stated that DISA was not offering the Thunderdome capabilities needed for DFAS as of December 2024. While the Thunderdome capabilities that DFAS needed may not be available yet, in feedback that DFAS received from the ZT PfMO on its implementation plan, the ZT PfMO stated, "Leveraging other agencies' solutions does not relieve the organization from providing an overall plan on ZT adoption."

(U) The Defense Media Activity ZT Implementation Plan Did Not Include All of the Required FY 2022 NDAA Elements

(U) The DMA CIO did not include all the FY 2022 NDAA-required elements in the DMA ZT implementation plan. Specifically, the DMA did not include the following elements in its ZT implementation plan.

¹⁵ (U) Some of the services that DISA provides to DFAS include: (1) Network Connection that enables the connections of computers, printers, routers, switches, and other devices used to communicate over various transmission media, such as the Defense Information Systems Network, which is the DoD's enterprise telecommunications network, and the DODIN; (2) Telecommunications that provide devices access to the Defense Information Systems Network for providing data, video, and voice services; (3) Database administration that includes labor support for the administration and sustainment of database operating environments; and (4) Cybersecurity Defense that provides protection for computers, networks, programs, and data from unintended or unauthorized access, change, or destruction by identifying, analyzing, and evaluating potential threats and preventing attacks.

- (U) Specific acquisitions, implementations, instrumentations, and operational workflows needed to implement ZT across unclassified and classified networks; operational technology; and weapon systems
- (U) Detailed schedule with target milestones and required expenditures
- (U) Interim and final metrics, including a phased migration plan
- (U) Identification of additional funding, authorities, and policies, as necessary

(U) The DMA CIO stated that the DMA ZT implementation plan did not include all FY 2022 NDAA elements because they did not have visibility of all DMA IT assets; therefore, they could not identify their IT acquisition needs. The DMA CIO stated that they were working with DISA to identify IT assets on several DMA networks but did not have an estimated time for completing this task.

(U) Having visibility over IT assets on an organization's network is the foundation for developing a cybersecurity program and implementing ZT. The lack of visibility of the DMA's assets limits the DMA CIO's ability to effectively identify the gaps in acquisitions, resources, and funding required for implementing ZT.

(U) The National Guard Bureau ZT Implementation Plan Did Not Include Any of the FY 2022 NDAA Elements and Was Not Submitted in a Timely Manner

(U) NGB officials did not submit the NGB ZT implementation plan to the ZT PfMO until February 5, 2024, 107 days after the October 21, 2023 due date. When submitted, the NGB ZT implementation plan did not include any of the FY 2022 NDAA required elements to include information about specific acquisitions, implementations, instrumentations, and operational workflows; a detailed schedule with target milestones; interim and final metrics, including a phased migration plan; or the identification of additional funding, authorities, and policies. According to the NGB Chief of Strategy and Governance, they did not initially submit an implementation plan because they received internal guidance stating that since the NGB mission-specific systems resided on the Army and Air Force networks, the NGB systems would be included in the Army and Air Force ZT implementation plans. On January 19, 2024, the NGB acknowledged that they needed to develop a separate ZT implementation plan and requested an extension to submit a plan. On February 5, 2024, the NGB submitted their plan, but as stated above, the plan did not include any of the FY 2022 NDAA required elements.

(U) In addition to revising the NGB implementation plan to include all required elements, the NGB needs to coordinate with the Army and Air Force to identify the ZT capabilities that the NGB will inherit from the Services.¹⁶ The NGB should identify the inherited capabilities in their ZT implementation plan to recognize that the Army and Air Force are responsible for implementing those capabilities for the NGB systems.

(U) The Defense Legal Services Agency Did Not Submit a ZT Implementation Plan

(U) DLSA officials did not submit a ZT implementation plan to the ZT PfMO. According to the DLSA IT Chief, the DLSA did not submit an implementation plan because they needed information from DISA, who provides network, database administration, and cybersecurity defense services, to complete their ZT implementation plan. Although ZT PfMO officials extended the deadline for the DLSA to submit their implementation plan to January 2024, the DLSA IT Chief elected to wait for the information needed from DISA to develop their plan. However, as of November 25, 2024, the DLSA has yet to submit a ZT implementation plan.

(U) Ensuring that ZT Implementation Plans Contain the Correct Information Is Critical

(U) Ensuring that ZT implementation plans contain complete information is critical to ensuring ZT implementation at all of the DoD Components. Submission of incomplete DoD Component ZT implementation plans limits the DoD's ability to address gaps in acquisition, funding, and policy to meet the ZT requirements in the FY 2022 NDAA and to track each DoD Component's progress toward meeting the FY 2027 deadline for ZT implementation.

(U) Management Comments on the Report and Our Response

(U) National Guard Bureau Comments

(U) The NGB CIO disagreed with the Finding, stating that they did not fail to communicate with the Army and Air Force regarding their ZT implementation plans and remained in contact with Army and Air Force representatives

¹⁶ (U) Capabilities are inherited when network, system, or application capabilities receives protection from security controls that are developed, implemented, assessed, authorized, and monitored by another internal or external organization where the system or application resides.

(U) throughout the process. The NGB CIO stated that the initial guidance was that the NGB did not need a ZT implementation plan because the NGB joint systems were owned by either the Army or the Air Force and would be included in their plans. The NGB CIO also stated that the ZT PfMO later provided clarifying guidance that the NGB needed to have a separate ZT implementation plan for the systems, regardless of system ownership, which resulted in the extensive delays in completing and submitting an implementation plan that included all the required FY 2022 NDAA elements.

(U) Our Response

(U) In the Finding section of this report, we state that the NGB failed to coordinate with the Army and Air Force regarding their ZT implementation plan for the NGB mission-specific systems; we did not state that the NGB failed to communicate with the Army and Air Force. The coordination is necessary for the NGB to determine the ZT capabilities that it will inherit from the Services so that the NGB can include those capabilities in its ZT implementation plan (Recommendation B.3.a). Based on the NGB CIO's comments, we revised the Finding to specify that the coordination is needed to determine the inherited capabilities.

(U) We also state in the Finding section that NGB officials believed that their systems would be included in the Army and Air Force's ZT implementation plans because the NGB mission-specific systems resided on the Army and Air Force networks. The initial guidance stating that the NGB did not need a ZT implementation plan did not originate from the ZT PfMO but from the Army and Air National Guard. Once the ZT PfMO learned that the NGB was not submitting a separate plan, they informed the NGB to submit a plan.

(U) Defense Information Systems Agency Director Comments

(U) Although not required to comment, the Director for DISA's Program Executive Office for Cyber, responding for the DISA Director, provided comments to the Background and Finding sections. The Director stated that there were instances in the report that implied Thunderdome was not yet available to DoD Components, although Thunderdome was in production as of February 2024. The Director stated that the audit report contained outdated information with respect to the number of ZT activities covered by Thunderdome and that the number of activities is subject to change in the near future. The Director also stated that the audit report contained outdated information with respect to DISA coordination with DFAS and DMA adding that DFAS is migrating to the Department of Defense Network, which will provide Thunderdome capabilities and that the DMA is working with the Thunderdome team for additional ZT assistance.

(U) Our Response

(U) We disagree that the report implies Thunderdome was not yet available to DoD Components. In the Background and Finding sections, we state that Thunderdome was being developed and, as of January 2025, it covered 85 of the 91 activities required to achieve target-level ZT. We also state in the DFAS section of the Finding, that “as of October 2024, DISA had developed a list of ZT capabilities that Thunderdome offers, which should allow DFAS to update their ZT implementation plan accordingly.” That statement indicates that Thunderdome was offering capabilities to the DoD Components by at least October 2024. With respect to DISA coordination with DFAS and DMA, the level of coordination stated in the report was identified by DFAS and DMA officials during the audit. We acknowledge that additional coordination with DFAS and DMA is occurring as indicated by the Director.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation B.1

~~(CUI)~~ We recommend that the Defense Finance and Accounting Service Director update and submit the Defense Finance and Accounting Service Zero Trust implementation plan to the DoD Chief Information Officer, to include the Defense Finance and Accounting Service [REDACTED].

(U) Defense Finance and Accounting Service Director Comments

~~(CUI)~~ The Director of Information and Technology, responding for the DFAS Director, agreed, stating that DFAS submitted updates to their ZT implementation plan in July 2024 and October 2024, which included [REDACTED].

(U) Our Response

~~(CUI)~~ Comments from the Director of Information and Technology addressed all specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Director provides a copy of their updated ZT implementation plan and we verify [REDACTED].

(U) Recommendation B.2

(U) We recommend that the Defense Media Activity Director:

- a. **(U) Develop a plan for identifying all Defense Media Activity network and system assets that includes metrics and milestones for completing the plan.**

(U) Defense Media Activity Director Comments

(U) The Acting DMA Director agreed, stating that the DMA identified its network and system assets and is currently focused on identifying the hardware and software inventory for each of those assets.

(U) Our Response

(U) Comments from the Acting DMA Director addressed all specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Acting DMA Director provides a copy of the plan and we verify that it provides instruction for identifying the DMA network and system assets along with metrics and milestones for completing the plan.

- b. **(U) Update and submit the Defense Media Activities Zero Trust implementation plan to the DoD Chief Information Officer, once all Defense Media Activity network and system assets are identified, to include the Defense Media Activity acquisition approach; implementation schedule; interim and final metrics, including a phased migration plan; and funding required for implementing zero trust.**

(U) Defense Media Activity Director Comments

(U) The Acting DMA Director agreed, stating that the DMA has attempted to secure resources for DISA's Thunderdome from DISA and was not successful. The Acting DMA Director stated that they are in the process of reaching out to the Acting DoD CIO to request assistance in writing a plan that would include the identification of funding required to implement ZT.

(U) Our Response

(U) Comments from the Acting DMA Director addressed all specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Acting DMA Director provides a copy of their updated ZT implementation plan and we verify that it was provided to the DoD CIO and includes an acquisition approach; implementation schedule; interim and final metrics, including a phased migration plan; and funding required to implement ZT.

(U) Recommendation B.3

(U) We recommend that the National Guard Bureau Chief:

- a. **(U) Coordinate with the Army and Air Force on the zero trust capabilities that the National Guard Bureau will inherit from the Services and update the National Guard Bureau Zero Trust implementation plan accordingly.**

(U) National Guard Bureau Chief Comments

(U) The NGB CIO, responding for the NGB Chief, agreed, stating that the NGB has confirmed that Army National Guard systems will be included in the Army's ZT implementation plan and Air National Guard systems will be included in the Air Force ZT implementation plans.

(U) Our Response

(U) Comments from the NGB CIO partially addressed the recommendation; therefore, the recommendation is unresolved. While the NGB confirmed that Army National Guard systems and Air National Guard systems will be included in the Army and Air Force ZT implementation plans, the NGB needs to coordinate with the Army and Air Force on the ZT capabilities that the NGB will inherit and must include those capabilities in the NGB ZT implementation plan. Therefore, we request that the NGB Chief provide additional comments within 30 days in response to the final report describing how the NGB will coordinate with the Army and Air Force to determine the ZT capabilities that the NGB will inherit and when it will update the NGB ZT implementation plan to include the inherited capabilities.

- b. **(U) Update and submit the National Guard Bureau Zero Trust implementation plan to the DoD Chief Information Officer, to include the National Guard Bureau acquisition approach, implementations, instrumentations, and operational workflows; a detailed schedule with target milestones; interim and final metrics, including a phased migration plan; and the identification of additional funding, authorities, and policies for implementing zero trust.**

(U) National Guard Bureau Chief Comments

(U) The NGB CIO, responding for the NGB Chief, agreed, stating that the NGB ZT implementation plan has been updated to include the missing elements identified in the report, and that the NGB continues to review its ZT implementation plan on an annual basis or when changes to the system inventory occur.

(U) Our Response

(U) Comments from the NGB CIO addressed all specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the NGB Chief provides a copy of the plan and we verify that it was provided to the DoD CIO and includes an acquisition approach, implementations, instrumentations, and operational workflows; a detailed schedule with target milestones; interim and final metrics, including a phased migration plan; and the identification of additional funding, authorities, and policies for implementing Zero Trust.

(U) Recommendation B.4

(U) We recommend that the Defense Legal Services Agency Director develop and submit a Zero Trust implementation plan to the DoD Chief Information Officer that includes an acquisition approach, implementations, instrumentations, and operational workflows; a detailed schedule with target milestones; interim and final metrics, including a phased migration plan; and the identification of additional funding, authorities, and policies for implementing zero trust.

(U) Defense Legal Services Agency Director Comments

(U) The Attorney-Manager for the DLSA, responding for the DLSA Director, agreed, stating that the DLSA provided the ZT PfMO the DLSA ZT implementation plan on December 6, 2024, that included details on the DLSA's strategy for ensuring target-level compliance for each ZT capability by the end of FY 2027. The Attorney-Manager also stated that the DLSA would address discrepancies in the DLSA ZT implementation plan to the DoD CIO's satisfaction by March 31, 2025.

(U) Our Response

(U) Comments from the Attorney-Manager addressed all specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the DLSA Director provides us a copy of the plan and we verify that it was provided to the DoD CIO and includes an acquisition approach, implementations, instrumentations, and operational workflows; a detailed schedule with target milestones; interim and final metrics, including a phased migration plan; and the identification of additional funding, authorities, and policies for implementing Zero Trust.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from January 2024 through December 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

(U) To determine whether the DoD complied with requirements to develop its ZT strategy, principles, architecture, and implementation plans in accordance with the FY 2022 NDAA, we analyzed the DoD's ZTRA, ZT Strategy, and Federal and DoD-wide guidance on ZT implementation. We also interviewed security managers and IT specialists, and we reviewed ZT implementation plans of select DoD Components to assess their completeness and to determine whether the plans included required FY 2022 NDAA elements. Furthermore, we interviewed officials from the following organizations to determine their roles and responsibilities as related to the DoD's ZT implementation.

- (U) Office of the DoD Chief Information Officer
- (U) DoD Zero Trust Portfolio Management Office
- (U) U.S. Cyber Command
- (U) Joint Force Headquarters-Department of Defense Information Network
- (U) Defense Information Systems Agency

(U) We selected the following DoD Components to ensure that we had a broad representation of DoD ZT implementation plans. Therefore, we selected 11 DoD Component-level ZT implementation plans to review from the 45 DoD Components required to submit an implementation plan. The Navy and Air Force each included another two plans with their implementation plans and, therefore, we reviewed a total of 15 plans.

- (U) U.S. Army
- (U) U.S. Navy (applies to the U.S. Marine Corps and U.S. Indo-Pacific Command)
- (U) U.S. Air Force (applies to the U.S. Space Command and U.S. Space Force)
- (U) National Guard Bureau

- (U) Defense Finance and Accounting Service
- (U) Defense Health Agency
- (U) Defense Information Systems Agency
- (U) Defense Legal Services Agency
- (U) Defense Threat Reduction Agency
- (U) Defense Media Activity
- (U) Office of Local Defense Community Cooperation

(U) We reviewed and assessed the ZT implementation plans that were submitted to the ZT PfMO to assess whether the plans included all ZT elements specified in the FY 2022 NDAA.

(U) Internal Control Assessment and Compliance

(U) We assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. In particular, we assessed the internal controls related to ensuring that the DoD complied with FY 2022 NDAA requirements to develop a ZT strategy, ZT principles, ZTRA, and ZT implementation plans. However, because our review was limited to this internal control component and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

(U) Use of Computer-Processed Data

(U) We did not use computer-processed data to perform this audit.

(U) Use of Technical Assistance

(U) The Quantitative Methods Division provided assistance in developing the methodology that we used to select the ZT implementation plans to assess the extent to which those plans included the ZT elements specified in the FY 2022 NDAA.

(U) Prior Coverage

(U) No prior coverage has been conducted on ZT during the last 5 years.

(U) Appendix B

(U) FY 2022 National Defense Authorization Act Zero Trust Requirements

135 STAT. 2044

PUBLIC LAW 117-81—DEC. 27, 2021

10 USC 2224
note.**SEC. 1528. ZERO TRUST STRATEGY, PRINCIPLES, MODEL ARCHITECTURE, AND IMPLEMENTATION PLANS.**

Deadline.

(a) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act, the Chief Information Officer of the Department of Defense and the Commander of United States Cyber Command shall jointly develop a zero trust strategy, principles, and a model architecture to be implemented across the Department of Defense Information Network, including classified networks, operational technology, and weapon systems.

(b) STRATEGY, PRINCIPLES, AND MODEL ARCHITECTURE ELEMENTS.—The zero trust strategy, principles, and model architecture required under subsection (a) shall include, at a minimum, the following elements:

(1) Prioritized policies and procedures for establishing implementations of mature zero trust enabling capabilities within on-premises, hybrid, and pure cloud environments, including access control policies that determine which persona or device shall have access to which resources and the following:

(A) Identity, credential, and access management.

(B) Macro and micro network segmentation, whether in virtual, logical, or physical environments.

(C) Traffic inspection.

(D) Application security and containment.

(E) Transmission, ingest, storage, and real-time analysis of cybersecurity metadata endpoints, networks, and storage devices.

(F) Data management, data rights management, and access controls.

(G) End-to-end encryption.

(H) User access and behavioral monitoring, logging, and analysis.

(I) Data loss detection and prevention methodologies.

(J) Least privilege, including system or network administrator privileges.

(K) Endpoint cybersecurity, including secure host, endpoint detection and response, and comply-to-connect requirements.

(L) Automation and orchestration.

(M) Configuration management of virtual machines, devices, servers, routers, and similar to be maintained on a single virtual device approved list (VDL).

(2) Policies specific to operational technology, critical data, infrastructures, weapon systems, and classified networks.

(3) Specification of enterprise-wide acquisitions of capabilities conducted or to be conducted pursuant to the policies referred to in paragraph (2).

(4) Specification of standard zero trust principles supporting reference architectures and metrics-based assessment plan.

(5) Roles, responsibilities, functions, and operational workflows of zero trust cybersecurity architecture and information technology personnel—

(A) at combatant commands, military services, and defense agencies; and

(B) Joint Forces Headquarters-Department of Defense Information Network.

(U) FY 2022 National Defense Authorization Act Zero Trust Requirements (cont'd)

PUBLIC LAW 117-81—DEC. 27, 2021

135 STAT. 2045

(c) ARCHITECTURE DEVELOPMENT AND IMPLEMENTATION.—In developing and implementing the zero trust strategy, principles, and model architecture required under subsection (a), the Chief Information Officer of the Department of Defense and the Commander of United States Cyber Command shall—

(1) coordinate with—

(A) the Principal Cyber Advisor to the Secretary of Defense;

(B) the Director of the National Security Agency Cybersecurity Directorate;

(C) the Director of the Defense Advanced Research Projects Agency;

(D) the Chief Information Officer of each military service;

(E) the Commanders of the cyber components of the military services;

(F) the Principal Cyber Advisor of each military service;

(G) the Chairman of the Joints Chiefs of Staff; and

(H) any other component of the Department of Defense as determined by the Chief Information Officer and the Commander;

Assessment.

(2) assess the utility of the Joint Regional Security Stacks, automated continuous endpoint monitoring program, assured compliance assessment solution, and each of the defenses at the Internet Access Points for their relevance and applicability to the zero trust architecture and opportunities for integration or divestment;

(3) employ all available resources, including online training, leveraging commercially available zero trust training material, and other Federal agency training, where feasible, to implement cybersecurity training on zero trust at the—

(A) executive level;

(B) cybersecurity professional or implementer level;

and

(C) general knowledge levels for Department of Defense users;

(4) facilitate cyber protection team and cybersecurity service provider threat hunting and discovery of novel adversary activity;

Assessment.

(5) assess and implement means to effect Joint Force Headquarters-Department of Defense Information Network's automated command and control of the entire Department of Defense Information Network;

Assessment.

(6) assess the potential of and, as appropriate, encourage, use of third-party cybersecurity-as-a-service models;

(7) engage with and conduct outreach to industry, academia, international partners, and other departments and agencies of the Federal Government on issues relating to deployment of zero trust architectures;

(U) FY 2022 National Defense Authorization Act Zero Trust Requirements (cont'd)

| | |
|------------------------|---|
| 135 STAT. 2046 | PUBLIC LAW 117-81—DEC. 27, 2021 |
| Assessment. Review. | <p>(8) assess the current Comply-to-Connect Plan; and</p> <p>(9) review past and conduct additional pilots to guide development, including—</p> <p>(A) utilization of networks designated for testing and accreditation under section 1658 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116-92; 10 U.S.C. 2224 note);</p> <p>(B) use of automated red team products for assessment of pilot architectures; and</p> <p>(C) accreditation of piloted cybersecurity products for enterprise use in accordance with the findings on enterprise accreditation standards conducted pursuant to section 1654 of such Act (Public Law 116-92).</p> |
| Deadline. | <p>(d) IMPLEMENTATION PLANS.—</p> <p>(1) IN GENERAL.—Not later than one year after the finalization of the zero trust strategy, principles, and model architecture required under subsection (a), the head of each military department and the head of each component of the Department of Defense shall transmit to the Chief Information Officer of the Department and the Commander of Joint Forces Headquarters-Department of Defense Information Network a draft plan to implement such zero trust strategy, principles, and model architecture across the networks of their respective components and military departments.</p> <p>(2) ELEMENTS.—Each implementation plan transmitted pursuant to paragraph (1) shall include, at a minimum, the following:</p> <p>(A) Specific acquisitions, implementations, instrumentations, and operational workflows to be implemented across unclassified and classified networks, operational technology, and weapon systems.</p> <p>(B) A detailed schedule with target milestones and required expenditures.</p> <p>(C) Interim and final metrics, including a phase migration plan.</p> <p>(D) Identification of additional funding, authorities, and policies, as may be required.</p> <p>(E) Requested waivers, exceptions to Department of Defense policy, and expected delays.</p> |
| Assessment. | <p>(e) IMPLEMENTATION OVERSIGHT.—</p> <p>(1) IN GENERAL.—The Chief Information Officer of the Department of Defense shall—</p> <p>(A) assess the implementation plans transmitted pursuant to subsection (d)(1) for—</p> <p>(i) adequacy and responsiveness to the zero trust strategy, principles, and model architecture required under subsection (a); and</p> <p>(ii) appropriate use of enterprise-wide acquisitions;</p> <p>(B) ensure, at a high level, the interoperability and compatibility of individual components' Solutions Architectures, including the leveraging of enterprise capabilities where appropriate through standards derivation, policy, and reviews;</p> <p>(C) use the annual investment guidance of the Chief to ensure appropriate implementation of such plans, including appropriate use of enterprise-wide acquisitions;</p> <p>(D) track use of waivers and exceptions to policy;</p> <p>(E) use the Cybersecurity Scorecard to track and drive</p> |

(U) FY 2022 National Defense Authorization Act Zero Trust Requirements (cont'd)

PUBLIC LAW 117-81—DEC. 27, 2021

135 STAT. 2047

implementation of Department components; and

(F) leverage the authorities of the Commander of Joint Forces Headquarters-Department of Defense Information Network and the Director of the Defense Information Systems Agency to begin implementation of such zero trust strategy, principles, and model architecture.

(2) ASSESSMENTS OF FUNDING.—Not later than March 31, 2024, and annually thereafter, each Principal Cyber Advisor of a military service shall include in the annual budget certification of such military service, as required by section 1657(d) of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116-92; 10 U.S.C. 391 note), an assessment of the adequacy of funding requested for each proposed budget for the purposes of carrying out the implementation plan for such military service under subsection (d)(1).

Deadline.
Assessment.

(f) INITIAL BRIEFINGS.—

(1) ON MODEL ARCHITECTURE.—Not later than 90 days after finalizing the zero trust strategy, principles, and model architecture required under subsection (a), the Chief Information Officer of the Department of Defense and the Commander of Joint Forces Headquarters-Department of Defense Information Network shall provide to the congressional defense committees a briefing on such zero trust strategy, principles, and model architecture.

(2) ON IMPLEMENTATION PLANS.—Not later than 90 days after the receipt by the Chief Information Officer of the Department of Defense of an implementation plan transmitted pursuant to subsection (d)(1), the secretary of a military department, in the case of an implementation plan pertaining to a military department or a military service, or the Chief Information Officer of the Department, in the case of an implementation plan pertaining to a remaining component of the Department, as the case may be, shall provide to the congressional defense committees a briefing on such implementation plan.

Deadline.

(g) ANNUAL BRIEFINGS.—Effective February 1, 2022, at each of the annual cybersecurity budget review briefings of the Chief Information Officer of the Department of Defense and the military services for congressional staff, until January 1, 2030, the Chief Information Officer and the head of each of the military services shall provide updates on the implementation in their respective networks of the zero trust strategy, principles, and model architecture.

Effective date.

(U) Appendix C

(U) DoD Zero Trust Component Implementation Plan Template

(U) The following table shows the ZT implementation plan Template alignment with the required FY 2022 NDAA ZT elements.

| (U) FY 2022 NDAA Elements for Component-Level Implementation Plans | DoD Zero Trust Component Implementation Plan Template Guidance |
|---|---|
| <p>Specific acquisitions, implementations, instrumentations, and operational workflows to be implemented across unclassified and classified networks; operational technology; and weapon systems*</p> | <p>Acquisitions</p> <ul style="list-style-type: none"> • High-level plan for acquiring ZT capabilities with the scope of the Component’s ZT implementation plan • Capabilities and activities, such as requirements, with solutions being currently implemented in the plan through FY 2027 • Delineation between solutions planned through enterprise-wide acquisitions and those planned through Component-level acquisitions and identification of potential gaps in people, processes, or technology • Acquisition-related industry engagements that are planned now or envisioned through FY 2027 • Alignment between Component-level ZT Acquisition Strategies, policies, and guidance |
| <p>Detailed schedule with target milestones and required expenditures</p> | <p>Key Milestones</p> <ul style="list-style-type: none"> • Provide a time-bound schedule for completion of critical events through FY 2027, including both applicable DoD-wide and Component-specific milestones related to ZT implementation, with an 18-month focus through March 2025. • Include resourcing decisions and deadlines; significant acquisition events; and major solution deployment milestones with other key execution milestones, such as start and completion dates of target-level ZT capabilities and activities, to demonstrate achievement of target level by FY 2027. • Include milestones for deployment and sunset of technologies. <p>Required Expenditures Address, at a high level, funding sources and status of ZT-related funding, including a detailed schedule of required expenditures.</p> <p style="text-align: right;">(U)</p> |

(U) DoD Zero Trust Component Implementation Plan Template (cont'd)

| <p>(U) FY 2022 NDAA Elements for Component-Level Implementation Plans</p> | <p align="center">DoD Zero Trust Component Implementation Plan Template Guidance</p> |
|--|---|
| <p>Interim and final metrics, including a phased migration plan</p> | <p>Interim Metrics, Final Metrics, and Phased Migration Plan Component ZT implementation plans will include interim and final metrics, including a phased migration plan. To meet these requirements, the following topic areas are recommended to be addressed.</p> <ul style="list-style-type: none"> • Specification of standard ZT principles supporting reference architectures and a metrics-based assessment plan • Current or intended Component measurement and reporting toward meeting the strategic goals outlined within the DoD ZT Strategy • Intended measurement toward implementation at the activity level |
| <p>Identification of additional funding, authorities, and policies, as necessary</p> | <p>Additional Funding, Authorities, and Policies Address, at a high level, funding sources and status of ZT-related funding.</p> <ul style="list-style-type: none"> • This section will address how the Component governs ZT Implementation; any planned policies or guidance; and “Identification of additional authorities, and policies, as should be required.” This will, at a high level, describe how the Component intends to oversee their planned implementation; how efforts and resources will be aligned, as applicable; how necessary governance decisions will be identified, addressed, or elevated; and how they interact with the existing DoD committee structures. • This section will also include planned policies and guidance developed at the Component level and any additional authorities or policies requiring action at a higher level to support implementation. |
| <p>Requested waivers, exceptions to DoD policies, and expected delays</p> | <p>Waivers, Exceptions, and Expected Delays Identify potential delays or exemptions to mandated timelines or requirements. Identify by name and provide justification for the following system occurrences.</p> <ul style="list-style-type: none"> • Delays – Any identified systems which will require an extension to mandated ZT timelines. • Exceptions – Any system identified for potential exception from ZT requirements. <p align="right">(U)</p> |

* (U) The DoD CIO did not develop policies specific to implementing ZT for operational technology and classified networks in accordance with the FY 2022 NDAA (as described in Finding A).

(U) Source: The ZT PfMO.

(U) Management Comments

(U) National Guard Bureau



NATIONAL GUARD BUREAU
111 SOUTH GEORGE MASON DRIVE
ARLINGTON, VA 22204-1373

NGB CIO/J6

13 FEB 25

MEMORANDUM FOR: DOD Inspector General

FROM: National Guard Bureau, Chief Information Officer/J6

SUBJECT: NGB Comments for "Draft Report for the Audit of the DoD's Compliance with the FY 2022 National Defense Authorization Act's Requirements Concerning Zero Trust (Report No. D2024-D000CR-0009.000)"

1. The statements below are comments provided in reference to the above-mentioned Draft Report regarding Zero Trust (ZT). Additional in-line comments have been provided within the attached draft report file titled "Draft Report of the D2024-D000CR-0009.000 - with NGB comments".

2. **NGB disagrees with Finding B regarding NGB.** NGB did not fail to communicate with the Army and Air Force regarding their ZT Implementation Plans as stated in the draft IG report. NGB has remained in contact with representatives from Army and Air Force throughout this process. The initial guidance was that a ZT Implementation Plan (I-Plan) was not required for NGB, as the NGB Joint systems were owned by either the Army or Air Force and therefore would fall under the purview of that parent service and their corresponding I-Plans. The DoD CIO ZT Portfolio Management Office (PfMO) later provided clarifying guidance that all systems listed within the NGB eMASS instance for joint systems would need to be part of a separate NGB I-Plan, regardless of system ownership. This background process led to the extensive delays in completing and submitting the I-Plan, as well as contributed to this initial version of the I-Plan not containing all required elements.

3. NGB agrees with Recommendation B.3.a. NGB has confirmed that all of ARNG will be incorporated into the Army's Unified Network plan and therefore is considered part of Army's I-Plan. ANG does not have separate IT systems, and ANG has confirmed that all its ZT efforts will fall under the Air Force I-Plan.

4. NGB agrees with Recommendation B.3.b and has already completed a revised ZT I-Plan that includes the missing elements identified in the draft IG report. NGB continues to review its ZT I-Plan on an annual basis or when changes to the system inventory occur. **NGB also notes that ZT PfMO efforts no longer focus on the actual Component Level I-Plan, but rather on a combination of the new PfMO-hosted and managed Data Metrics Collection System and additional PfMO-issued taskers in ETMS2.** The Data Metrics Collection System is used to generate reports on Component ZT progress. All information regarding ZT compliance, funding, and

(U) National Guard Bureau (cont'd)

NGB-CIO/J6

SUBJECT: NGB Comments for "Draft Report for the Audit of the DoD's Compliance with the FY 2022 National Defense Authorization Act's Requirements Concerning Zero Trust (Report No. D2024-D000CR-0009.000)"

scheduling for each NGB system is located within the Data Metrics Collection System and updated on a quarterly basis, or when otherwise directed by ZT PfMO.

5. NGB has satisfied all the requirements put forth by the ZT PfMO during calendar year 2024 for data calls, implementation updates, and details on NGB ZT strategy, planning, and funding. NGB stays in regular contact with ZT PfMO representatives regarding NGB's plans and processes for ensuring NGB systems achieve the target-level requirements by the end of FY'27, as directed.

6. NGB CIO/J6 acknowledges and agrees to the release of CUI to Congress as outlined in the above-mentioned draft report, provided corrections are made to address the factual errors with Finding B as outlined above and in the attached draft report with comments.

7. For questions regarding this memo please contact [REDACTED], NGB J6 ZT AO Lead, at [REDACTED] or [REDACTED].

MCNEILL, KENNETH H. CHRISTOPHER
HER
Date: 2025.02.13 10:09:01 -0500

KENNETH C. MCNEILL
Chief Information Officer/J6
National Guard Bureau

(U) DoD Chief Information Officer



CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

FEB 21 2025

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Review and Comment on the DoD Inspector General’s Draft Report “Audit of the DoD’s Compliance with the National Defense Authorization Act for Fiscal Year 2022’s Requirements Concerning Zero Trust” (D2024-D000CR-0009.000).

The Department of Defense (DoD) Chief Information Officer (CIO) responds in this document to the DoD Inspector General’s (IG) Draft Report, Audit of the DoD’s Compliance with the National Defense Authorization Act for Fiscal Year (FY) 2022’s Requirements Concerning Zero Trust” (D2024-D000CR-0009.000). The DoD CIO directed the Zero Trust (ZT) Program Management Office (PfMO) under the Deputy DoD CIO for Cybersecurity to ensure that all requirements set forth in the DODIG recommendations are met and actions are taken that will satisfy closure of any/all open or unresolved recommendations.

DoD IG RECOMMENDATION A.1: The DoD Chief Information Officer should establish and implement a plan for accelerating the development of new policies and revision to existing policies specific to implementing the Zero Trust framework on operational technology, infrastructures, and weapon systems, including milestones for completion of those policies.

DoD CIO RESPONSE: The DoD CIO agrees with the DoD IG’s recommendation. The ZT PfMO created and implemented an accelerated ZT Policy Playbook with Plan of Action and Milestones (POA&M), both attached. The Playbook and POA&M will accelerate policy issuance and include milestones for developing new and revising existing policies. The DoD CIO has been collaborating closely with OUSD (A&S) since February 2024, engaging subject matter experts to best inform the ZT Portfolio Management Office on the implementation of the Zero Trust on Operational Technology, Infrastructures, and Weapon Systems, including milestones for completion of forthcoming ZT PfMO guidance. The DOD CIO will continue to prioritize establishment of the ZT policies and guidance for Operational Technology guidance by December 2025. Recognizing the complex nature of Infrastructures and Weapons Systems, the DoD CIO, OUSD (A&S), The Joint Chiefs of Staff, and Military Services are further committed to establishing proper ZT guidance by December 2026.

My point of contact for this matter is [REDACTED] She can be reached at [REDACTED] or [REDACTED].

Leslie A. Beavers
Leslie A. Beavers
Acting

Attachments:
As stated

(U) Defense Finance and Accounting Service



DEFENSE FINANCE AND ACCOUNTING SERVICE
8899 EAST 56TH STREET
INDIANAPOLIS, IN 46249-0201

February 14, 2025

MEMORANDUM FOR Program Director for Audit Cyber Operations, Department of Defense (DoD) Office of Inspector General (IG)

SUBJECT: DFAS-Information & Technology Management Comments to DoD IG Draft report “Audit of the DoD’s Compliance with the FY 2022 National Defense Authorization Act’s Requirements Concerning Zero Trust,” (Project No. D2024-D000CR-0009.000), dated January 22, 2025.

In accordance with the subject audit, attached are management comments to the Draft report for recommendation(s). DFAS concurs with B.1 recommendation contained in the DoD IG report based on the initial DFAS Zero Trust implementation plan (iPlan) submission in October 2023.

DFAS has reviewed the draft report and has no changes to the DoD IG classification or markings.

DFAS acknowledges that our Component’s Controlled Unclassified Information will be released to Congress.

My point of contact is [REDACTED], ([REDACTED]) [REDACTED], [REDACTED].

MEANS.LLEWELLY | Digitally signed by
MEANS.LLEWELLY.N.D.JR [REDACTED]
N.D.JR [REDACTED] | Date: 2025.02.18 17:30:55 -05'00'

L. Don Means Jr
Director, Information & Technology

Attachment:
As stated

Proudly Serving America’s Heroes
www.dfas.mil

(U) Defense Information Systems Agency

~~CUI~~

DoD ISSUANCE COORDINATION RESPONSE

COMPONENT COORDINATOR RESPONSE

February 18, 2025

SUBJECT: Administrative Instruction for review of DoDIG Draft Report for the audit of the DOD's compliance with the FY 2022 National Defense Authorization Act's Requirements Concerning Zero Trust (Report No: D2024-DOOOCR 0009.00)

On behalf of my Component, my formal response to this issuance is: Concur with comment. Below are comments for your consideration.

My point of contact for this action is [REDACTED]

| | | |
|---|--------------------|---------------------------------|
| X | HERMANN.BRIAN | Digitally signed by |
| | GUSTAV. [REDACTED] | HERMANN.BRIAN.GUSTAV [REDACTED] |
| | | Date: 2025.02.21 16:52:18 -0500 |

Double-click the 'X' to insert a digital signat...
or print and sign a hard copy.

Coordinating Official's Name: Brian G. Hermann
Coordinating Official's Position Title: Director
Coordinating Official's Component: DISA PEO Cyber

DD FORM 818, AUG 2016 SELECT A CLASSIFICATION

(U) Defense Information Systems Agency (cont'd)

| SELECT A CLASSIFICATION | | | | | | |
|---|---|------|-------------------|--------------------------|--|---|
| DoD ISSUANCE COORDINATION RESPONSE: Issuance Type and Number, "Title" | | | | | | |
| CLASS | # | PAGE | PARA | BASIS FOR NON-CONCUR? | COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION | COMPONENT AND POC NAME, PHONE, AND E-MAIL |
| U | | 5 | 2 | <input type="checkbox"/> | <p>Coordinator Comment and Justification: Paragraph states the following " (U) In support of the DoD's ZT implementation, the Defense Information Systems Agency (DISA) is developing an enterprise ZT solution, known as Thunderdome, that is intended to be available to DoD Components to secure access to applications and data; protect enclaves; and protect applications operating in a cloud environment or on-premises. According to DISA, Thunderdome will include a suite of IT and cyber-based technologies that will leverage enterprise identity and access management"</p> <p>Coordinator Recommended Change: This language indicates future state as in "is developing", "is intended to be available", "will include". TD is an operational capability in production today in both IL5/IL6 CONUS and OCONUS. Components can deploy TD capabilities today so please revise to correct current tense.</p> <p>Originator Response: Partially accept. See reasoning.</p> <p>Originator Reasoning: See above</p> | <p>Brian Hermann DISA PEO Cyber [Redacted] Office: [Redacted]</p> |
| U | | 10 | Table 2, Column 2 | <input type="checkbox"/> | <p>Coordinator Comment and Justification: Paragraph states "(U) Thunderdome is designed to cover 85 of 91 activities required to achieve target-level ZT. DoD Components that have systems that are not on the DoD Network are responsible for identifying and implementing a ZT solution of their choice but have the option to purchase Thunderdome services from DISA"</p> <p>Coordinator Recommended Change: This number is outdated based on initial RFI collection and subject to change in the near future based on final TSMO assessment report.</p> | <p>Brian Hermann DISA PEO Cyber [Redacted] Office: [Redacted]</p> |

DD FORM 818, AUG 2016

REPLACES SD FORM 818, WHICH IS OBSOLETE

SELECT A CLASSIFICATION

(U) Defense Information Systems Agency (cont'd)

| SELECT A CLASSIFICATION | | | | | | |
|---|---|-------|---------|--------------------------|--|---|
| DoD ISSUANCE COORDINATION RESPONSE: Issuance Type and Number, "Title" | | | | | | |
| CLASS | # | PAGE | PARA | BASIS FOR NON-CONCUR? | COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION | COMPONENT AND POC NAME, PHONE, AND E-MAIL |
| | | | | | <p>Originator Response: Partially accept. See reasoning.</p> <p>Originator Reasoning: See above</p> | |
| U | | 15-19 | Various | <input type="checkbox"/> | <p>Coordinator Comment and Justification: Although DISA's I-Plan was considered sufficient in the audit, a number of organizations reference a dependency on DISA in their I-Plan deficiencies (DFAS, DLSA, DMA) . This information may be outdated based on time of initial RFI.</p> <p>Coordinator Recommended Change: Note that DFAS is currently working migration to DODNET which will provide TD capabilities and is assessing mission environment options for applications/workloads. DMA is also working with the J6/TD teams on migration planning and additional ZT assistance. The TD team at this time has not had any direct engagement requests from DLSA team on ZT requirements. These comments are not for DISA action in this report but noting updates.</p> <p>Originator Response: Partially accept. See reasoning.</p> <p>Originator Reasoning: See above</p> | <p>Brian Hermann DISA PEO Cyber [REDACTED] Office: [REDACTED]</p> |

(U) Defense Information Systems Agency (cont'd)

SELECT A CLASSIFICATION

DoD ISSUANCE COORDINATION RESPONSE: Issuance Type and Number, "Title"

HOW TO FILL OUT THE DD 818 MATRIX

GENERAL GUIDANCE:

- **To sort table** by page/paragraph number, hover your mouse over the top of the first cell in the "page" column until a downward arrow appears; click and drag to the right to select both page and para columns. Under Paragraph on the Home ribbon, select A-Z button, set to sort by Column 3 and then Column 4, and select "OK." **To add new rows**, copy and paste a blank row to keep consistent formatting. **To add automatic numbering to column 2**, select entire column and click on the Numbering button under Paragraph on the Home ribbon.

COORDINATING OSD AND DOD COMPONENTS:

- Do not use the DD Form 818-1.
- Fill in the memo indicating your Component's position on the issuance. Fill in the authorized coordinator's name, position, and Component. The authorized coordinator (digitally) signs the response after the comment matrix has been completed. **Making additional changes after filling in a digital signature invalidates and removes the signature.**
- Use the comment matrix to provide comments to the OSD Component that created the issuance. Complete the header and footer and Columns 1 -7:
 - COLUMN 1* Enter the classification of the comment. If any material is **classified**, follow DoDM 5200.01 guidance for marking the document. If all comments are unclassified, mark the header and footer and ignore the column.
 - COLUMN 2* Order comments by the pages/paragraphs that they apply to in Columns 3 and 4.
 - COLUMNS 3&4* Cite the page on which the paragraph appears; cite the paragraph number as it appears in the text, e.g. 2.1.a..
 - COLUMNS 5* Only mark this box if you non-concur with the issuance and the comment in the applicable row is part of the basis for that non-concur. A nonconcur is typically used only when an issuance contains: (a) a violation of the law or contradiction of Executive Branch policy or of existing policy in a DoDD, DoDI, or other instrument approved by the Secretary or Deputy Secretary of Defense; or (b) an unnecessary risk to safety, life, limb, or DoD materiel; waste or abuse of DoD appropriations; or unreasonable burden on a DoD Component's resources.
 - COLUMN 6* Place only one comment per row. Enter your comment, justification, and recommended changes in the first two areas provided. If any material is **classified** or **controlled unclassified information**, follow DoDM 5200.01 or DoDI 5200.48 guidance for marking the document.
 - COLUMN 7* As stated.
- **Review** the comments, **resolve** any conflicting views, and **confirm** that the completed matrix accurately represents your Component's position. Upload the form to the DoD Directives Program Portal in **Microsoft Word format (.docx)**, with the signed memo representing your Component's position.

DD FORM 818, AUG 2016

REPLACES SD FORM 818, WHICH IS OBSOLETE

SELECT A CLASSIFICATION

4

(U) Defense Legal Services Agency



**DEPARTMENT OF DEFENSE
OFFICE OF GENERAL COUNSEL**
1600 DEFENSE PENTAGON
WASHINGTON, DC 20301-1600

MEMORANDUM FOR CYBERSPACE OPERATIONS, DOD OFFICE OF INSPECTOR
GENERAL

SUBJECT: DLSA Response to the Draft Audit of DoD’s Compliance with the FY 2022
National Defense Authorization Act’s Requirements Concerning Zero Trust

The Defense Legal Services Agency (DLSA) agrees with recommendations outlined in the draft Audit Report on DoD’s Compliance with the FY 2022 National Defense Authorization Act’s Requirements Concerning Zero Trust; Project No. D2024-D000CR-0009.000.

Specifically, these recommendations require DLSA to develop and submit a Zero Trust (ZT) implementation plan to the DoD Chief Information Officer, that includes an acquisition approach, implementations, instrumentations, and operational workflows; a detailed schedule with target milestones; interim and final metrics, including a phased migration plan; and the identification of additional funding, authorities, and policies for implementing zero trust.

Although not detailed in the draft report, the DLSA ZT implementation plan was provided to the DoD CIO on 6 December 2024. This comprehensive plan details DLSA’s ZT Strategy for ensuring target-level compliance for each ZT capability by the end of FY 2027. DLSA is committed to addressing any discrepancies within the ZT Implementation Plan to DOD CIO’s satisfaction by 31 March 2025.

Further, DLSA has reviewed the draft report for the presence of CUI content and has determined that the respective DLSA portions do not contain CUI material.

Point of contact for this memorandum is the DLSA ZT Lead [REDACTED], [REDACTED].

HARVEY.BRENT Digitally signed by
HARVEY.BRENT [REDACTED]
Date: 2025.02.21 13:20:32
-05'00'

Brent. C. Harvey
Attorney-Manager



(U) Defense Media Activity



~~CUI~~
DEPARTMENT OF DEFENSE
DEFENSE MEDIA ACTIVITY
6700 TAYLOR AVENUE, SUITE 5902
FORT MEADE, MD 20755

February 24, 2025

MEMORANDUM FOR THE INSPECTOR GENERAL

SUBJECT: Audit of the DoD's Compliance with the FY 2022 National Defense Authorization Act's Requirements Concerning Zero Trust (Project No. D2024-D000CR-0009.000)

DMA management concurs with the draft DOD IG report without comment.

Actions taken to address the recommendations to date are:

B.2.a. (U) Develop a plan for identifying all Defense Media Activity network and system assets that includes metrics and milestones for completing the plan.

- DMA has identified the networks and systems that make up the IT Portfolio of our component, we are currently focusing on RMF Step 1 identifying the assets: Hardware/Software/PPSM inventory of each.

B.2.b. (U) Update and submit the Defense Media Activities Zero Trust implementation plan to the DoD Chief Information Officer, once all Defense Media Activity network and system assets are identified, to include the Defense Media Activity acquisition approach; implementation schedule; interim and final metrics, including a phased migration plan; and funding required for implementing Zero Trust.

- DMA participated with the DOD CIO in the FY24 ZT Issue paper attempting to secure resources to acquire Thunderdome from DISA for all networks/systems not transitioning to DoDnet in FY25, we were not successful in that endeavor.

- DMA director is reaching out to [REDACTED] to request assistance in writing the plan which would include identifying funding.

LEDERER.MAX
DONALD.JR. Digitally signed by
LEDERER.MAX.DONALD.J
Date: 2025.02.24
13:48:54 -05'00'

Max A Lederer
Acting Director

(U) Acronyms and Abbreviations

- (U) CIO** Chief Information Officer
- (U) DFAS** Defense Finance Accounting Service
- (U) DISA** Defense Information Systems Agency
- (U) DLSA** Defense Legal Services Agency
- (U) DMA** Defense Media Activity
- (U) IT** Information Technology
- (U) NDAA** National Defense Authorization Act
- (U) NGB** National Guard Bureau
- (U) ZT** Zero Trust
- (U) ZT PfMO** Zero Trust Portfolio Management Office
- (U) ZTRA** Zero Trust Reference Architecture

Whistleblower Protection

U.S. DEPARTMENT OF DEFENSE

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

For more information about DoD OIG reports or activities, please contact us:

Legislative Affairs Division
703.604.8324

Public Affairs Division
public.affairs@dodig.mil; 703.604.8324



www.dodig.mil

DoD Hotline
www.dodig.mil/hotline



~~CUI~~



DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098

~~CUI~~