



DEPARTMENT OF DEFENSE

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

July 17, 2025

Incorporating Change 1, September 2, 2025

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Directive-Type Memorandum 25-003, “Implementing the DoD Zero Trust Strategy”

References: See Attachment 1.

Purpose. In accordance with the authority in DoD Directive 5144.02, this directive-type memorandum:

- Establishes the Zero Trust (ZT) Portfolio Management Office (PfMO) and describes its responsibilities to coordinate, synchronize, and accelerate the DoD Enterprise’s adoption of ZT architecture and cybersecurity framework, modernizing the DoD’s ability to impede malicious threat actors in cyberspace. A detailed overview of the ZT PfMO is in Attachment 3.
- Establishes the position of Chief ZT Officer and outlines roles and responsibilities, as determined by the CIO, to orchestrate DoD-wide ZT execution, including providing strategic guidance, directing the alignment of efforts, and recommending resource and funding prioritization to advance ZT adoption across the DoD in alignment with the DoD ZT Strategy.
- Is effective July 17, 2025; it will be converted into a DoD instruction. This DTM will expire effective July 17, 2026.

Applicability. This issuance applies to OSD, the Military Departments (including the U.S. Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies and DoD Field Activities (DAFAs), and all other organizational entities within the DoD (referred to collectively in this issuance as the “DoD Components”).

Definitions. See Glossary.

Responsibilities. See Attachment 2.

Summary of Change 1. This administrative change corrects acronyms.

Releasability. Cleared for public release. Available on the Directives Division Website at <https://www.esd.whs.mil/DD/>.

A handwritten signature in blue ink, appearing to read 'Keh', with a long horizontal stroke extending to the right.

Katherine Arrington
Performing the Duties of DoD Chief
Information Officer

Attachments
As stated

ATTACHMENT 1

REFERENCES

DoD Cyber Council Charter, March 21, 2023

DoD Directive 5105.79, “DoD Senior Governance Framework,” November 8, 2021

DoD Directive 5144.02, “DoD Chief Information Officer (DoD CIO),” November 21, 2014,
as amended

DoD Instruction 4120.24, “Defense Standardization Program,” March 31, 2022

DoD Instruction 5025.01, “DoD Issuances Program,” August 1, 2016, as amended

DoD Zero Trust Strategy, October 21, 2022¹

Executive Order 12333, “United States Intelligence Activities,” December 4, 1981

Public Law 113-283, “Federal Information Security Modernization Act,” December 18, 2024

United States Code, Title 10

United States Code, Title 40

United States Code, Title 50

¹ Available at <https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf>

ATTACHMENT 2

RESPONSIBILITIES

1. DOD CHIEF INFORMATION OFFICER (DOD CIO). The DoD CIO:

a. Provides the foundation and the direction to align ongoing and future ZT-related cybersecurity efforts, investments, and initiatives across all elements of doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P).

b. Serves as Co-Chair of the DoD ZT Executive Committee (EXCOM). Oversees implementation, coordination and alignment across the DoD and Intelligence Community (IC) of the DoD ZT Strategy within existing committee structures.

c. Designates a DoD civilian, no lower than a Senior Executive Service level or equivalent, to serve as the Chief ZT Officer as described in this issuance.

d. In coordination with the Commander, United States Cyber Command (CDRUSCYBERCOM):

(1) Oversees implementation of the DoD ZT Strategy within existing committee structures.

(2) Annually reviews and assesses:

(a) DoD Component ZT implementation plans (I-Plans) for how the DoD ZT strategy, principles, framework, and architecture are applied and implemented across their networks (including all infrastructure and systems to include Defense Critical Infrastructure and weapon system (WS)).

(b) The feasibility, executability, acceptability, suitability, and expected cybersecurity outcomes (based on the ZT capability and outcome of descriptions) of such plans.

e. Utilizes the DoD Cybersecurity Hardening Scorecard located in Secure Internet Protocol Router Network (<https://intelshare.intelink.sgov.gov/sites/CS-Scorecard>) to track and drive DoD ZT Strategy, implementation requirements, progress, and assessed and realized security outcomes. Other reporting mechanisms (e.g., reporting in accordance with Public Law 113-283, also known as the “Federal Information Security Modernization Act”) must also be leveraged as appropriate.

2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). Under the authority, direction, and control of the DoD CIO, and in addition to the responsibilities in Paragraph 11., the Director, DISA:

a. Aligns (and adjusts as needed) enterprise services to address DoD-wide adoption of ZT.

b. Includes DoD ZT planning into DISA's I-Plan and further synchronizes and aligns I-Plan execution to support DAFA unclassified and classified networks that DISA protects.

c. Requires enterprise services provided to DoD Components comply with and deliver certain redundant and resilient ZT capabilities.

d. Incorporates ZT principles, as outlined in the DoD Zero Trust Strategy, into existing DISA-provided cybersecurity training.

e. In the capacity of Commander, Department of Defense Cyber Defense Command (CDRDCDC), serves as a Co-Chair of the DoD ZT EXCOM.

3. UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING (USD(R&E)). The USD(R&E):

a. Incorporates ZT requirements into policy, guidance, and training related to:

(1) Research.

(2) Systems engineering.

(3) Manufacturing.

(4) Test and evaluation strategy and planning development.

(5) Technology development, innovation, and protection activities and programs, including development and approval of science and technology protection and program protection plans.

(6) Development and approval of verification, validation, and accreditation of models, simulations, distributed simulations, and their associated data.

(7) Independent technical risk assessments.

b. Assesses incorporation of ZT principles in major defense acquisition category identification programs when:

(1) Conducting independent technical risk assessments in accordance with Section 4272b of Title 10, United States Code (U.S.C.).

(2) Conducting developmental test and evaluation sufficiency assessments.

(3) Reviewing and approving science and technology protection plans, program protection plans, and developmental test and evaluation plans or strategies.

c. Promotes standardization of ZT practices through the Defense Standardization Program in accordance with DoD Instruction 4120.24.

d. Manages the DoD science and technology enterprise portfolio to address near-term and far-term ZT capability against emerging threats.

e. Maintains the DoD Joint Federated Assurance Center to develop and provide assurance capabilities and expertise, including capabilities that support ZT.

f. Serves as a member of the DoD ZT EXCOM.

4. UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT (USD(A&S)). The USD(A&S):

a. In collaboration with DoD Component heads, assesses the feasibility, limitations, and benefits of applying ZT principles and objectives in WS and defense critical infrastructure in acquisition and sustainment phases.

b. Incorporates ZT strategic principles and objectives into:

(1) DoD-wide acquisition strategies, policies, frameworks, Supply Chain Risk Management, and directives, as appropriate.

(2) DoD-wide defense critical infrastructure related acquisition policies and directives (e.g., Operational Technology, Internet of Things, Industrial Control Systems), as appropriate.

(3) DoD weapon- and weapons systems-related acquisition policies and directives, as applicable.

c. Serves as a member of the DoD ZT EXCOM.

5. PRESIDENT, DEFENSE ACQUISITION UNIVERSITY. Under the authority, direction, and control of the USD(A&S), the President, Defense Acquisition University:

a. Develops and makes accessible a standard set of tiered ZT training courses to be adopted across the DoD.

b. Provides DoD Components with training support in the integration of ZT into their acquisition and cybersecurity processes.

6. ASSISTANT SECRETARY OF DEFENSE FOR CYBER POLICY (ASD(CP)). Under the authority, direction, and control of the Under Secretary of Defense for Policy and in the capacity of the DoD Principal Cyber Advisor (PCA), the ASD(CP) serves as a member of the DoD ZT EXCOM.

7. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS (USD(P&R)). The USD(P&R):

- a. Aligns, coordinates, adjusts and implements enterprise services necessary policies, guidance, resourcing, human capital management, business IT services, measures and assessments to address DoD-wide adoption of ZT.
- b. Provides coordination, alignment and implementation of measures, assessments, training, professional descriptions, professional standards and operational qualifications as they relate and defined within the DoD to support adoption of ZT.
- c. Serves as a member of the DoD ZT EXCOM.

8. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (USD(I&S)). In coordination with the DoD CIO and the respective IC Chief Information Officer (CIO), the USD(I&S):

- a. Ensures ZT interoperability in accordance with Titles 10 and 50, U.S.C. for the DoD intelligence mission area.
- b. Collaborates with the DoD CIO and the IC CIO in aligning and deconflicting IC ZT guidance and metrics.
- c. Ensures DoD and IC ZT metrics satisfy the cybersecurity and information needs of both DoD and IC CIOs.
- d. Highlights gaps and overlaps in DoD and IC ZT implementations.
- e. Represents DoD intelligence mission area in DoD and IC ZT oversight forums.
- f. Serves as a member of the DoD ZT EXCOM.

9. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE (NSA/CSS). Under the authority, direction, and control of the USD(I&S); the authority, direction, and control exercised by the DoD CIO over the activities of the Cybersecurity Directorate, or any successor organization, of the NSA, funded through the Information System Security Program; and in addition to the responsibilities in Paragraph 11., the Director, NSA/Chief, CSS:

- a. Provides innovative and technical support to the DoD ZT PfMO in its mission to achieve the DoD's goal of reaching target level ZT by 2027. Ensures close collaboration and coordination between the DoD ZT PfMO and the NSA/CSS ZT team, to achieve clear and measurable objectives. These activities include, but are not limited to:

(1) Conducting no less than six PfMO-approved ZT technical assistance engagements per fiscal year (FY) across the DoD to support the DoD's goal of achieving target level ZT by 2027.

(2) Sustaining ZT implementation and modernization technical assistance and guidance support to the DoD Components annually on an as needed basis.

b. Provides technical guidance and expertise in support of the DoD ZT PfMO activities to include subject matter expert support to PfMO staff, technical research, lessons learned from engagements, and collaboration on technical artifacts (e.g., cybersecurity information sheets), to support the DoD's goal of achieving target level ZT by 2027. Such support includes technical guidance and expertise involving:

(1) ZT.

(2) Artificial Intelligence and Machine Learning.

(3) Cloud.

(4) Database.

(5) Web Development.

(6) Networking:

(a) System Administration.

(b) Operational system expertise.

(c) Other ZT related skill sets as required.

c. Builds, operates, and sustains one unclassified DoD ZT testbed (to the advanced ZT level), with the ability to provide comprehensive tenant hosting, to support:

(1) Enterprise system modeling.

(2) Evaluation of ZT solutions, enablers, and assessment tools.

(3) PfMO identified and approved ZT proof of concepts. Examples include:

(a) Automated ZT functional assessment (ZTFA) tools.

(b) Virtualized storage and services projection to support the PfMO in developing the ZTFA.

(c) Cooperative vendor software as a service integrations and interoperability testing.

(d) Canonical controlled vocabularies and tagging and labeling interoperability testing.

(4) Other PfMO-identified innovation and experimentation activities, as needed.

d. Supports the PfMO in developing a ZTFA process.

e. Serves as a member of the DoD ZT EXCOM.

10. CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER (CDAO). In coordination with the DoD CIO, the CDAO:

a. Develops and publishes enterprise-wide data tagging standards that support ZT adoption and DoD and IC data tagging interoperability across their ZT infrastructures.

b. Develops, publishes, and updates enterprise-wide policy and guidance for data, analytics, visualization, and artificial intelligence as it pertains to ZT implementation.

c. Provides oversight for use and implementation of enterprise analytic tools to support initial automation of data categorization and security responses, focusing on tagging and managing access to sensitive data and information.

d. In coordination with the Chief ZT Officer, ensures enterprise data policy accommodates ZT data tagging and labeling needs, including machine-readable attributes, data, and data models.

e. Serves as a member of the DoD ZT EXCOM.

11. DOD COMPONENT HEADS. The DoD Component heads:

a. Achieve, at minimum, target level ZT across all unclassified and classified systems (including national security systems) on the Department of Defense Information Network (DoDIN), with priority of effort on the Nonclassified Internet Protocol Router Network and the SECRET Internet Protocol Router Network by the end of FY 2027, in accordance with the DoD ZT Strategy and all associated implementation guidance.

b. Incorporate ZT principles into:

(1) Component-specific defense critical infrastructure requirements.

(2) Data, applications, assets, and services in weapons systems at the combined joint tactical environment to ensure data and information are appropriately secured in denied, degraded, intermittent, and limited bandwidth environments.

c. Address all dimensions of DOTMLPF-P in the design, development, deployment, and implementation of ZT capabilities and account for changes and additions on how each element impacts the DoD Components' ZT implementation.

d. Submit Component-level ZT I-Plans annually to the DoD CIO through the ZT PfMO (and CDRUSCYBERCOM through the CDRDCDC) and update subsections of these plans as may be required by the ZT PfMO. On an annual basis within their ZT I-Plans, submit any request for ZT implementation deviations, exceptions, or delays to the ZT PfMO for DoD CIO consideration.

(1) Include a plan of action and milestones with any request for deviation, exception, or delay.

(2) Submit requests for implementation deviations to the ZT PfMO quarterly, if necessary and required.

e. Incorporate ZT requirements into Component-specific acquisition strategies, policies, frameworks, and directives.

f. Identify personnel whose positions require additional or specialized ZT training.

g. Encourage personnel to take ZT training. Update other cybersecurity training courses and classes, based on mission need, to include ZT cybersecurity practices, principles, frameworks, architectures, and outcomes.

h. Provide data upon request to support ZT implementation metrics as identified by the ZT PfMO within ZT I-Plan guidance and the DoD Cybersecurity Hardening Scorecard.

i. Require DoD Cyber Assessment Teams, which combines the offensive tactics of a Red Team with the defensive strategies of a Blue Team, to evaluate ZT environments. Final reports must identify the level of ZT achieved and summarize the effectiveness of preventing an adversary from impacting DoD mission critical data.

j. Serve as a member of the DoD ZT EXCOM.

12. CDRUSCYBERCOM. In addition to the responsibilities in Paragraph 11., the CDRUSCYBERCOM:

a. Incorporates ZT principles in the development of strategy, doctrine, tactics, and training for cyber operations activities.

b. Addresses ZT equities for aligned forces.

c. Reviews cyberspace operations forces readiness metrics to ensure inclusion of ZT principles and activities, as appropriate. Reviews cyberspace operations forces training to identify changes to existing training or new training needed on ZT and coordinates requirements with the Military Services for inclusion in their I-Plans.

d. Ensures that the DoDIN Operations Center maintains the capability for automated data aggregation and visibility across DoDIN areas of operation to:

(1) Enable situational understanding and command and control of DoDIN Operations and Defensive Cyberspace Operations – Internal Defensive Measures.

(2) Counter adversary activity on the DoDIN.

e. Serves as a member of the DoD ZT EXCOM.

f. Through the CDRDCDC and in coordination with the DoD CIO and the DoD ZT EXCOM:

(1) Oversees implementation of the DoD ZT Strategy.

(2) Reviews and assesses DoD Component ZT I-Plans for how the DoD ZT strategy, principles, and model architecture are applied across their networks (including all infrastructure and systems) and the feasibility, executability, acceptability, suitability, and expected security outcomes (based on the ZT capability and outcome descriptions) of such plans.

13. ASSISTANT SECRETARY OF DEFENSE FOR SPECIAL OPERATIONS AND LOW-INTENSITY CONFLICT. In coordination with the DoD CIO, USD(A&S), CDAO, and Director of Operational Test and Evaluation, the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict:

a. Provides oversight for use and implementation of enterprise analytic tools to support initial automation of data categorization and security responses, focusing on tagging and managing access to sensitive data and information.

b. Ensures enterprise data policy accommodates ZT data tagging and labeling needs, including machine-readable attributes, data, and data models.

c. Ensures ZT interoperability in accordance with Title 10, U.S.C. and Title 50, U.S.C. for the DoD special operations mission area.

d. Issues, reviews, and approves United States Special Operations Command (USSOCOM) ZT guidance on shared networks.

e. Ensures USSOCOM ZT metrics satisfy the cybersecurity, and information needs of the CIO, NSA, and United States Cyber Command.

f. Represents USSOCOM mission area in DoD ZT oversight forums.

ATTACHMENT 3

ZT PfMO

1. PURPOSE. This attachment delineates Chief ZT Officer and ZT PfMO authorities and specific responsibilities.
2. APPLICABILITY. This attachment applies to the Chief ZT Officer, ZT PfMO, assigned staff, and supporting entities.
3. MISSION. The ZT PfMO is the overall DoD ZT lead to coordinate, synchronize, and advance the DoD Enterprise into a ZT cybersecurity architecture, modernizing the DoD's ability to prevent malicious actors from exploiting DoD data and resources.
4. AUTHORITIES. The Chief ZT Officer:
 - a. Has authorities delegated from the DoD CIO to execute all assigned missions and responsibilities.
 - b. Acts pursuant to the authorities and direction of the DoD Cyber Council and the DoD ZT EXCOM, while elevating key decisions as necessary across all dimensions of DOTMLPF-P impacted by ZT.
 - c. Sets the direction, strategy, execution milestones, and processes for implementation of the DoD ZT Strategy DoD-wide.
 - d. Develops, issues, and tracks DoD-wide ZT-related governance decisions (including roles and responsibilities), processes, and guidance. As necessary, develops DoD policy and implementing guidance for DoD CIO action in accordance with DoD Instruction 5025.01.
 - e. Serves as the coordinator for ZT efforts and supports the DoD Cyber Council regarding all matters related to ZT implementation. ZT PfMO guidance must align with all applicable DoD CIO and, when appropriate, Director of National Intelligence governance and directives.
 - f. Serves as the key authority for any ZT-related task, engagement, briefing, or report to or from Congress.
 - g. Oversees the resourcing and recommends priority alignment of DoD Component ZT funding necessary to successfully implement the stated goals of the DoD ZT Strategy.

h. Interfaces with, orchestrates, and accelerates ZT adoption across the DoD with key stakeholders, including:

(1) Federal Government partners: Executive Office of the President, Office of Management and Budget, the IC, and Federal Civilian Executive Branch agencies.

(2) Industry.

(3) Academia.

(4) Research Labs (including University Affiliated Research Centers and Federally Funded Research and Development Centers).

(5) Foreign partners and coalition allies.

5. CHIEF ZT OFFICER RESPONSIBILITIES.

a. ZT Strategy and Planning.

(1) Publishes and, as necessary, updates the DoD ZT Strategy and associated execution plans and roadmap(s).

(2) Reviews and approves DoD Component-level ZT I-Plans and associated roadmaps.

(3) Sets DoD enterprise strategic and execution milestones and definitions for achievement of:

(a) DoD ZT target capabilities.

(b) DoD ZT advanced capabilities.

(4) Ensures ZT-related budgets are properly synchronized and aligned with the achievement of DoD target level ZT and DoD advanced level ZT, as applicable, to achieve the stated outcomes of target level ZT before the end of FY 2027.

(5) Prioritizes DoD ZT resources within existing DoD CIO Capability Programming Guidance in accordance with Section 11319 of Title 40, U.S.C. and other policies. Reprioritizes ZT resources, if necessary, with the aid of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense and Director of Cost Assessment and Program Evaluation to achieve target level ZT before the end of FY 2027.

(6) Supports annual ZT funding assessments and advises on DoD Component ZT budget planning.

(7) Maintains awareness of DoD-wide budgetary actions that impact adoption of ZT across the DoD.

(8) Supports the DoD Cyber Council and DoD ZT EXCOM regarding all matters related to ZT implementation.

(9) Brings other non-technical decisions to the applicable DoD governance forum or DoD CIO committees.

b. ZT Portfolio and Risk Management.

(1) Defines, coordinates and, as necessary, publishes DoD ZT guidance.

(2) Manages, governs, and prioritizes the DoD ZT portfolio of initiatives and actions implementing the DoD ZT Strategy.

(3) Defines and monitors DoD ZT enterprise risks and mitigation strategies.

(4) Develops, issues, and tracks ZT-related governance decisions (including roles and responsibilities) and processes for the DoD.

(5) Defines and publishes ZT strategy, execution, and capability and activity metrics.

(6) Approves and publishes DoD ZT assessment guidance and guidance documents.

(7) Tracks progress and verifies DoD Components have completed the actions outlined in DoD ZT strategy, policies, and standards.

(8) Monitors Federal regulations, directives, and laws that could impact implementation of the DoD ZT Strategy.

c. ZT Architecture and Technical Support.

(1) Provides DoD ZT technical advisory and support, including test plans towards pilots and exercises to evaluate ZT capabilities and solutions.

(2) Defines and publishes DoD ZT requirements.

(3) Reviews and provides input to reference DoD ZT architectures and interrelated reference architectures and design documentation (e.g., cybersecurity reference architecture).

(4) Ensures interoperability of DoD Component and other mission partner ZT architectures.

(5) Review DoD Component evidence of technical achievement of ZT target capabilities and ZT advanced capabilities.

d. ZT Operations.

(1) Publishes tailored ZT communications for both internal and external DoD consumption.

(2) Builds and sustains a DoD ZT community of practice.

(3) Oversees and provides input to the development and implementation of DoD ZT training.

(4) Consults and coordinates with ZT stakeholders and partners.

(5) Develops, issues, updates, and tracks ZT-related governance decisions (including roles and responsibilities) and processes for the DoD.

(6) Develops ZT-related policy recommendations for DoD CIO approval.

ATTACHMENT 4

DOD ZT EXCOM

1. PURPOSE. This attachment delineates DoD ZT EXCOM authorities, structure, and specific responsibilities.
2. APPLICABILITY. This attachment applies to DoD Components, assigned staff, and supporting entities.
3. AUTHORITIES. The DoD ZT EXCOM is established pursuant to the authorities of the DoD CIO to orchestrate implementation of the DoD ZT Strategy and the DoD Cyber Council, the primary authority for ZT technical and strategic direction. The DoD Cyber Council is Co-Chaired by the DoD CIO and DoD PCA on behalf of the Deputy Secretary of Defense. DoD ZT EXCOM-specific responsibilities do not alter or supersede any existing authority or policy.
4. STRUCTURE. The Co-Chairs and members of the DoD ZT EXCOM will be represented at the general officer/flag officer or Senior Executive Service level. DoD CIO advisors and representatives from DAFAs other than those specifically listed in Paragraphs 4.a. and 4.b. of this attachment may attend upon invitation from the Co-Chairs. The ZT PfMO will serve as the Secretariat. DoD ZT EXCOM structure, processes, and operating procedures will be further developed in its charter and are subject to change based on the mission and leadership guidance.
 - a. Co-Chairs:
 - (1) DoD CIO.
 - (2) Director, DISA.
 - b. Members:
 - (1) USD(R&E).
 - (2) USD(A&S).
 - (3) DoD PCA.
 - (4) USD(P&R).
 - (5) USD(I&S).
 - (6) Director, NSA/Chief, CSS.
 - (7) CDAO.

(8) DoD Component heads:

- (a) Deputy Secretary of Defense.
- (b) Chairman of the Joint Chiefs of Staff.
- (c) Combatant Commanders.
- (d) Inspector General of the Department of Defense.
- (e) Secretaries of the Military Departments.
- (f) Commandant, United States Coast Guard.
- (g) DAFA Directors.
- (h) Chief, National Guard Bureau.

(9) Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense.

(10) Director, Cost Assessment and Program Evaluation.

(11) Director of Operational Test and Evaluation.

(12) CDRUSCYBERCOM.

(13) Representatives from:

(a) Joint Staff Command, Control, Communications and Computers/Cyber Directorate (J6).

(b) Joint Staff Force Structure, Resource, and Assessment Directorate (J8).

(c) Department of the Army CIO.

(d) Department of Navy CIO.

(e) Department of Air Force CIO.

(f) Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict.

5. RESPONSIBILITIES. The DoD ZT EXCOM is a senior-level governance oversight body to facilitate adaptive and timely implementation and decision making to achieve the DoD ZT Strategy and to accelerate ZT adoption across the DoD. The DoD ZT EXCOM:

a. Provides senior-level direction and resolves any and all issues threatening the successful implementation of the DoD ZT Strategy that do not require elevation to entities chartered in accordance with DoD Directive 5105.79 or other DoD CIO committee structures.

b. Provides executive level oversight to the strategy, principles, frameworks, and implementations related to ZT adoption.

c. Increases collaboration among DoD Components in achieving ZT across the DoD Information Enterprise, to include:

(1) All unclassified and classified systems (including national security systems) on the DoDIN, with priority of effort on the Nonclassified Internet Protocol Router Network and the SECRET Internet Protocol Router Network.

(2) Defense critical infrastructure (e.g., operational technology, Internet of Things, ICS, Supervisory Control and Data Acquisition).

(3) Data, applications, assets, and services in WS and at the tactical edge to ensure information is appropriately secured in denied, degraded, intermittent, and limited bandwidth environments.

(4) All dimensions of DOTMLPF-P in the design, development, deployment, and operations of ZT capabilities.

d. Identifies any topics outside the DoD ZT EXCOM's purview to be addressed at the appropriate forum(s).

e. Meets quarterly, or as required, to resolve issues quickly and adaptively to accelerate ZT adoption.

f. Provides regular updates regarding implementation of the DoD ZT Strategy to other senior leaders and governance bodies, when necessary.

GLOSSARYPART I. ACRONYMS

ACRONYM	MEANING
CDAO	Chief Digital and Artificial Intelligence Officer
CDRDCDC	Commander, Department of Defense Cyber Defense Command
CDRUSCYBERCOM	Commander, United States Cyber Command
CIO	chief information officer
CSS	Central Security Service
DAFA	Defense Agency and DoD Field Activity
DISA	Defense Information Systems Agency
DoD CIO	DoD Chief Information Officer
DODIN	Department of Defense Information Network
DOTMLPF-P	doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy
EXCOM	executive committee
FY	fiscal year
IC	Intelligence Community
I-Plan	implementation plan
NSA	National Security Agency
PCA	Principal Cyber Advisor
PfMO	Portfolio Management Office
U.S.C.	United States Code
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USD(R&E)	Under Secretary of Defense for Research and Engineering
USSOCOM	United States Special Operations Command
WS	weapon system
ZT	Zero Trust
ZTFA	Zero Trust functional assessment

PART II. DEFINITIONS

TERM	DEFINITION
advanced level ZT	Defined in the DoD Zero Trust Strategy.
canonical controlled vocabularies	An authoritative single term that is mapped to a moderately atomic, scientifically defensible, non-collided, non-deviated definition, based on a DoD enterprise principle or rule.
IC	Defined in Executive Order 12333.
target level ZT	Defined in the DoD Zero Trust Strategy.