



# DoD Information Enterprise - Zero Trust Framework



- › Secure information at all operational levels
- › Create dynamic access control capabilities
  - › Interoperate with secured data
- › Automate cyber and ZT with AI

**DOD INFORMATION SYSTEMS  
SECURED & DEFENDED**



Full interoperation of DoD cybersecurity and Zero Trust practices achieve enterprise resilience and protection

**TECHNOLOGY ACCELERATION**



Deploy Zero Trust technologies equal to or exceeding industry advancements outpacing the changing threat environment

- › Continually update & advance ZT enabled IT
- › Virtualize and breakdown silos
- › Simplify architectures
- › Automate data management

**ZERO TRUST CULTURAL ADOPTION**



A Zero Trust security framework and mindset that guides the design, development, integration, and deployment of access control and data protection across the DoD Enterprise Ecosystem

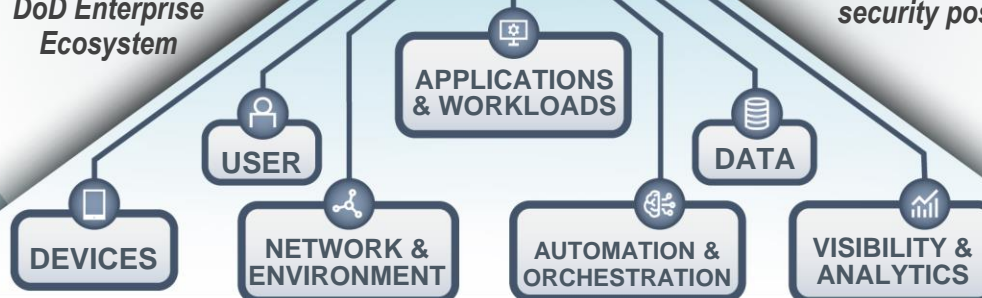
- › A workforce that embraces ZT
- › Increased collaboration and productivity
- › Increased commitment to ZT cybersecurity



**ZERO TRUST ENABLEMENT**

DoD Zero Trust permeates Department-level and Component-level processes resulting in seamless and coordinated security posture

- › Native operations and performance
- › Consistent, aligned, and effectively resourced ZT supporting functions
- › Streamline and accelerate acquisition processes to deploy ZT capabilities



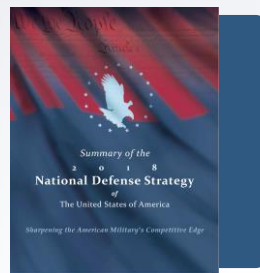


# DoD Information Enterprise - Zero Trust Guidance



## STRATEGIC GUIDANCE

- EO 14028, "Improving the Nation's Cybersecurity" (21 May 2021)
- National Defense Authorization Act for FY 2022 (27 Dec 2021)
- OMB M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles" (26 Jan 2022)
- NMM-2022-01, "National Security Memorandum 8, Zero Trust Security and Cloud Migration Security Guidance" (2 Feb 2022)
- National Defense Strategy (28 Mar 2022)



## DOD ZT CAPABILITIES

Capabilities define the outcomes that Components must reach to achieve minimum ZT Target & Advanced Level capabilities.

Capability	Category	Priority	Target Level	Advanced Level
1. Identity and Access Management	Identity	High	Yes	Yes
2. Device and Network Security	Network	High	Yes	Yes
3. Data Protection and Privacy	Data	High	Yes	Yes
4. Application Security	Application	High	Yes	Yes
5. Cloud Security	Cloud	High	Yes	Yes
6. Incident Response and Recovery	Incident Response	High	Yes	Yes
7. Security Awareness and Training	Security Awareness	High	Yes	Yes
8. Risk Management	Risk Management	High	Yes	Yes
9. Compliance and Governance	Compliance	High	Yes	Yes
10. Security Architecture	Security Architecture	High	Yes	Yes

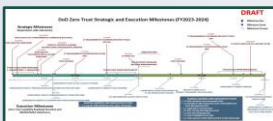
## ZT CAPABILITY TIMELINES

Roadmap depictions show how Zero Trust capabilities will advance across the 7 pillars.



## ZT IMPLEMENTATION MILESTONES

Specified milestones provide a basis to guide implementation planning activities.



## DOD ZT STRATEGY

Establishes desired outcomes for Components to achieve minimum ZT Target Level capabilities across the DoD Information Enterprise (IE) for data, assets, applications, services (DAAS) at all classification levels.



## DOD ZT REFERENCE ARCHITECTURE

Establishes a framework that provides guidance via architectural Pillars and Principles and identifies which of the overall strategic needs (goals and objectives) are the focus of the Reference Architecture.