DoD Zero Trust Portfolio Management Office

Theater Session on Zero Trust at AFCEA TechNet Cyber

Col Gary R. Kipe
Deputy Director, DoD ZT Portfolio Management Office (ZT PfMO)
May 4, 2023

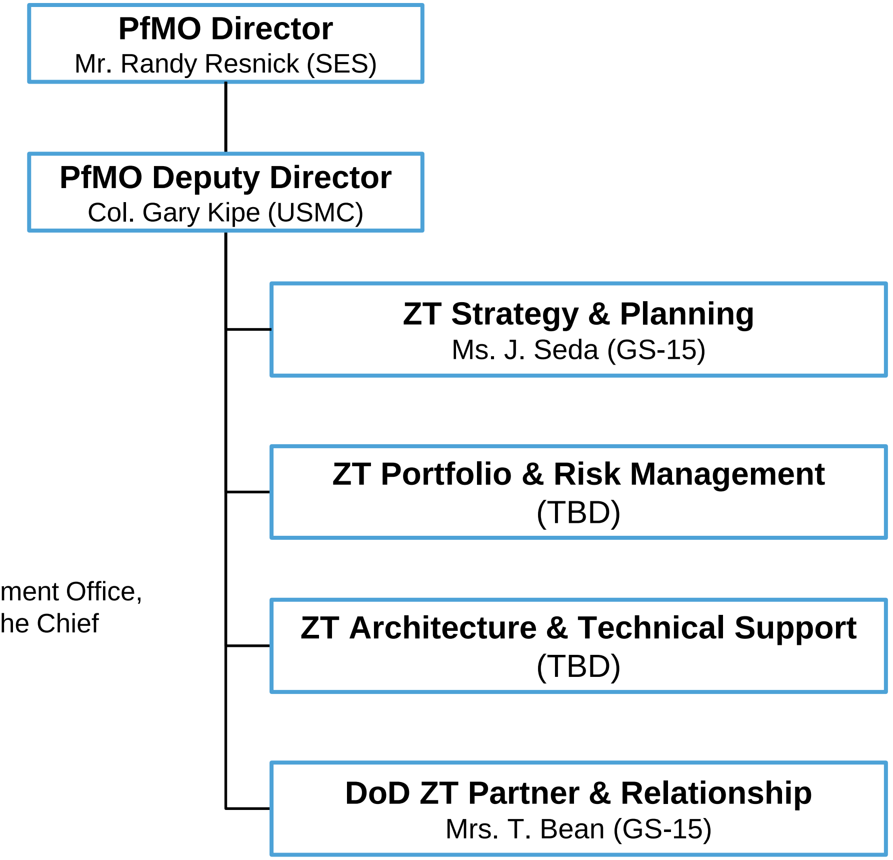
Outline

Intent: Explain the DoD's ZT approach to *accelerate* ZT adoption and implementation within the DoD

- High-level overview of DoD ZT PfMO, approach, strategic guidance, and DoD ZT implementation process model (via ZT Activities and ZT Capabilities)
- Review FY23 ZT pilot efforts
- Review DoD ZT Training Courses/Initiatives
- Review 18-month ZT PfMO Summary View
- Questions

The DoD CIO established the ZT PfMO to accelerate ZT adoption at the Department-level

The ZT PfMO is the lead for the DoD to coordinate, synchronize, and accelerate the DoD Enterprise to a ZT architecture, transforming the Department's ability to defend against malicious actors in cyberspace.



PfMO Director
Mr. Randy Resnick (SES)

PfMO Deputy Director
Col. Gary Kipe (USMC)

ZT Strategy & Planning
Ms. J. Seda (GS-15)

ZT Portfolio & Risk Management
(TBD)

ZT Architecture & Technical Support
(TBD)

DoD ZT Partner & Relationship
Mrs. T. Bean (GS-15)

Randy Resnick
Director, Zero Trust Portfolio Management Office, Department of Defense Office of the Chief Information Officer

ZT PfMO Roles

- Focal Point for ZT Knowledge
- Capability Enhancement
- ZT Guidance "Gaps"
- Embracing Talent
- Effective Support
- Centralized Role
- Strategic Communications

The Core Functions of the DoD ZT PfMO

- **Focal Point for ZT Knowledge** – Principal point for collecting and sharing ZT best practices, drawing on expertise and experiences across the ecosystem, Industry, Services, Agencies and DAFA's

- **Capability Enhancement** – Mission to raise ZT capability, knowledge and understanding across Department

- **ZT Guidance** – Produce authoritative Department ZT Strategy that is supported by appropriately aligned and enforced policies and directives, with a view of overall DoD risks and threats

- **Embracing Talent** – Need to identify and develop a cadre of ZT professionals across the DoD enterprise

- **Effective Support** – Deliver ZT support, strategy and visibility to DoD leadership

- **Centralized Role** – There is a need for a centralized entity to accelerate ZT adoption across the Department, under the DoD CIO, empowered to champion, defend, and orchestrate ZT-related programmatic and technical activities for the Department

- **Strategic Communications** – Develop and communicate the Zero Trust Vision, Strategy and Implementation Plan for the Department, and to communicate these efforts across the DoD, 5-eyes, NATO, Fed/Civ, as necessary and required

DoD’s Critical Path Forward to ZT Adoption

Strategic Guidance

PUBLIC LAW 117–81—DEC. 27, 2021 135 STAT. 1541

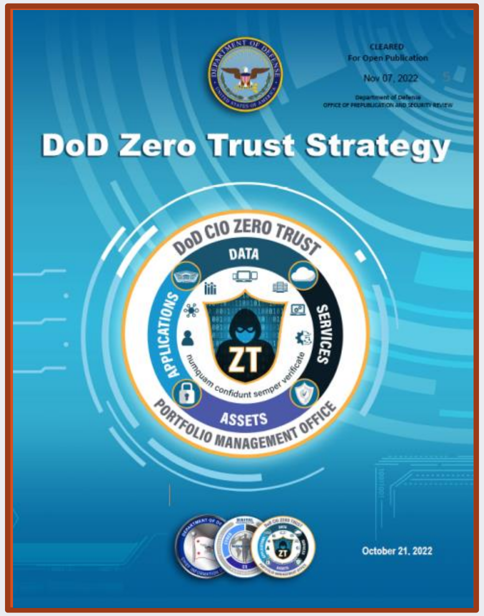
Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intellig

EXECUTIVE OFFICE OF THE PRESIDENT

National Cybersecurity Strategy

- **EO 14028**, “Improving the Nation’s Cybersecurity” (21 May 2021)
- **N**ational **D**efense **A**uthorization **A**ct 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** (22 Mar 2022)
- **National Cybersecurity Strategy** (1 Mar 2023)

DoD ZT Strategy



CLEARED
For Open Publication
Nov 07, 2022
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

DoD Zero Trust Strategy

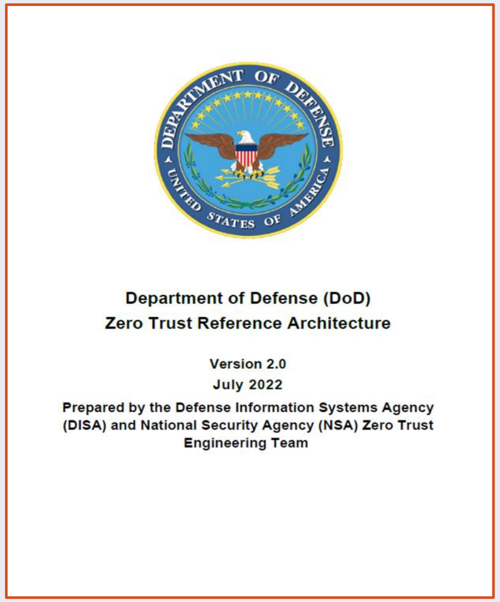
DoD CIO ZERO TRUST
DATA
SERVICES
ASSETS
APPLICATIONS
ZT
numquam confidunt semper verificate
PORTFOLIO MANAGEMENT OFFICE

October 21, 2022

21 October 2022:
Establishes desired outcomes for Components to achieve “ZT Target Level” capabilities and activities across the DoD Information Enterprise (IE) for data, assets, applications and services (DAAS) on DoD Information Network.

Link HERE

DoD ZT Reference Architecture



Department of Defense (DoD)
Zero Trust Reference Architecture

Version 2.0
July 2022

Prepared by the Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team

July 2022:
The Zero Trust Reference Architecture (v2.0) is the Departments authoritative source of information about ZT that guides and constrains the instantiations of multiple DoD ZT architectures and potential solutions.

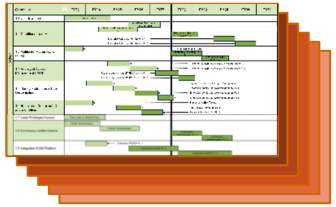
Link HERE

DoD ZT Capabilities

DoD Zero Trust Capabilities (45)

Capabilities define the Activity outcomes that Components must reach to achieve Target & Advance Levels of Zero Trust.

ZT Capability and Activity Timelines



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

Implementation Milestones

Specified (and implied) target milestones provide a basis to guide implementation planning activities.

ZT Capabilities Link HERE
ZT Roadmap Link HERE

Overall strategic vision and outcomes for accelerating ZT adoption by FY27

DOD Zero Trust Strategic Vision

A DoD Information Enterprise secured by a fully implemented, Department-wide Zero Trust cybersecurity framework.

- The Department requires a scalable, resilient, auditable and defendable environment centered on securing and protecting all data, application, assets, and services (DAAS) in cyberspace.
- The DoD ZT Strategy establishes the goals and objectives to implement within the five-year planning and budgeting horizon.

Strategic Intent

- Accelerate the move to a data cybersecurity paradigm (versus primarily perimeter-based).
- Adoption of Zero Trust cybersecurity results in an effective set of checks and balances. DoD users located anywhere are confident that the data accessed, the assets deployed, the applications used, and the services provided are secure & resilient.
- This enables DoD and Mission Partners to access data where they have the need to know based on least privilege.

Strategic Outcome

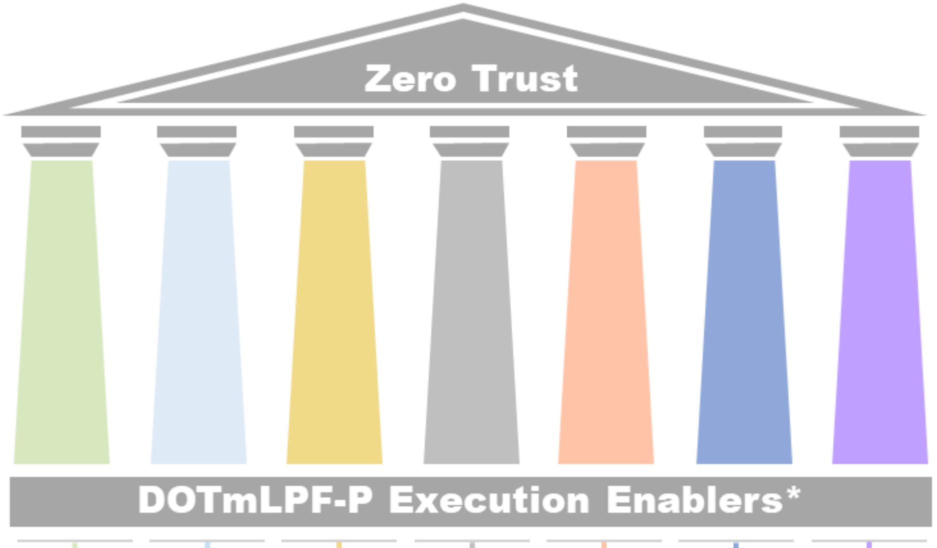
Bottom Line: ***Stop adversaries*** from exploiting the DoDIN and stealing our data.

DoD ZT Strategy provides strategic direction

What We Will Achieve	Vision	*A DoD Information Enterprise secured by a fully implemented, Department-wide Zero Trust cybersecurity framework*			
		What We Understand & Agree To	What to "Do"	How to "Do" Zero Trust	What Support is Needed
	Goals	**1. Zero Trust Cultural Adoption** *A Zero Trust security framework and mindset that guides the design, development, integration, and deployment of information technology across the DoD Zero Trust Ecosystem*	**2. DoD Information Systems Secured & Defended** *DoD cybersecurity practices incorporate and operationalize Zero Trust to achieve enterprise resilience in DoD information systems*	**3. Technology Acceleration** *Zero Trust-based technologies deploy at a pace equal to or exceeding industry advancements to remain ahead of the changing threat environment*	**4. Zero Trust Enablement** *DoD Zero Trust execution integrates with Department-level and Component-level processes resulting in a seamless and coordinated ZT execution*
How We Realize That Value	Objectives	1.1 Commitment	2.1 User	3.1 Capabilities	4.1 Policy
		1.2 Outreach	2.2 Device	3.2 Architecture	4.2 Programming
		1.3 Awareness	2.3 Application & Workload	3.3 Interoperability	4.3 Planning
		1.4 Workforce	2.4 Data	3.4 Ideation / Innovation	4.4 Funding
		1.5 Training	2.5 Network & Environment		4.5 Acquisition
			2.6 Automation & Orchestration		4.6 Performance
			2.7 Visibility & Analytics		4.7 Zero Trust PfMO

* *Extracted from DoD Zero Trust Strategy, v1, 21 Oct 2022, p. vi*

DoD Zero Trust pillars and enablers provide the foundation for implementing ZT



Zero Trust

DOTmLPF-P Execution Enablers*

User

Continually authenticate, access, and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions.

Devices

Understanding the health and status of devices informs risk decisions. Real time inspection, assessment and patching informs every access request.

Applications & Workloads

Secure everything from Applications to hypervisors, to include the protection of containers and virtual machines.

Data

Data transparency and visibility enabled and secured by enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging.

Network & Environment

Segment, isolate and control (physically and logically) the network environment with granular policy and access controls.

Automation & Orchestration

Automated security response based on defined processes and security policies enabled by AI, e.g., blocking actions or forcing remediation based on intelligent decisions.

Visibility & Analytics

Analyze events, activities and behaviors to derive context and apply AI/ML to achieve a highly personalized model that improves detection and reaction time in making real-time access decisions.

Enablers: *The design, development, deployment, and operations of ZT capabilities must account for changes and/or additions to how DoD Components execute ZT across elements of* ***D****octrine,* ***O****rganization,* ***T****raining,* ***m****aterial,* ***L****eadership &* ***E****ducation,* ***P****ersonnel,* ***F****acilities, and* ***P****olicy.*

DoD Zero Trust Capabilities (45)

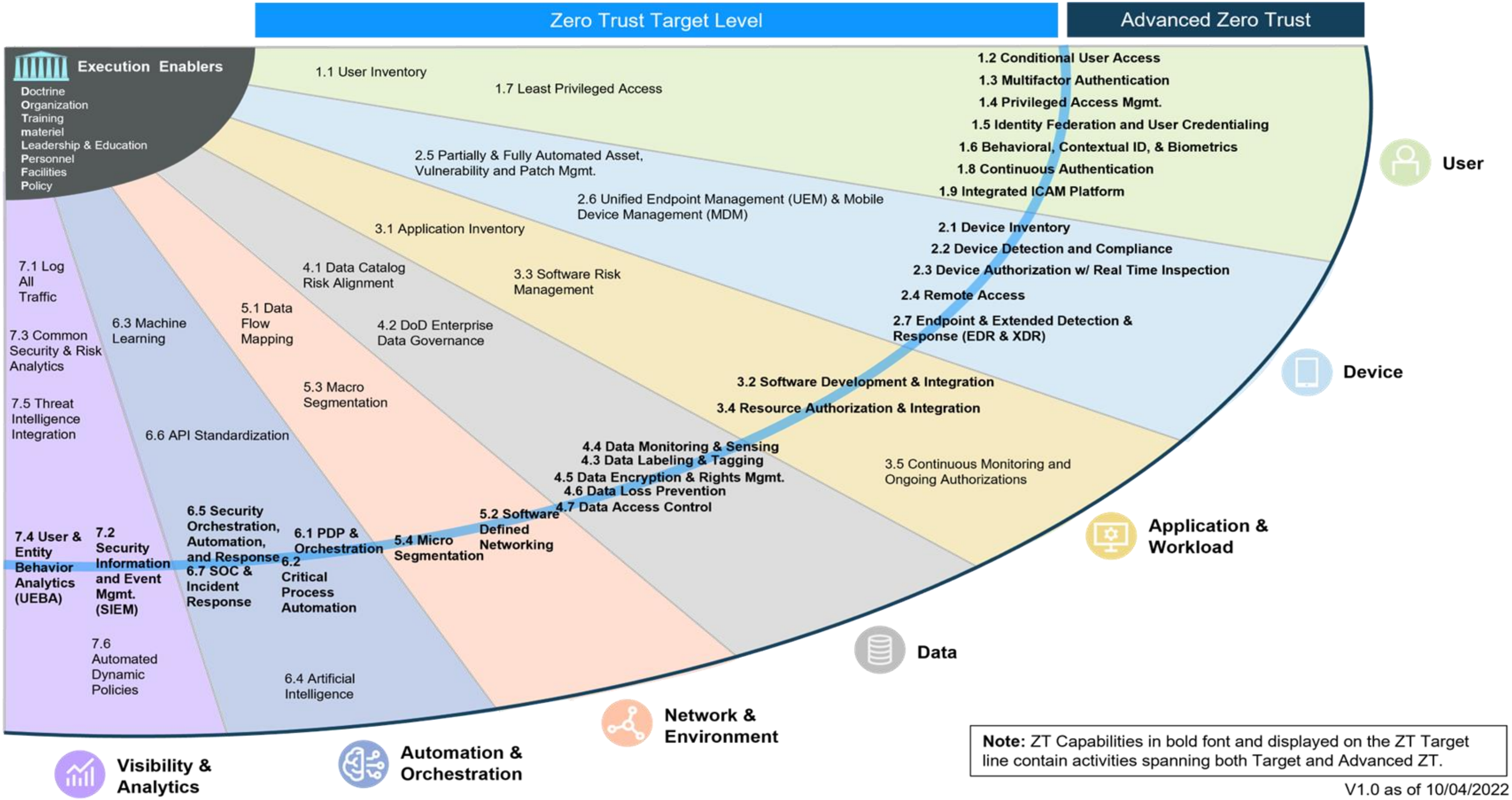
User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
1.1 User Inventory	**2.1** Device Inventory	**3.1** Application Inventory	**4.1** Data Catalog Risk Assessment	**5.1** Data Flow Mapping	**6.1** Policy Decision Point (PDP) & Policy Orchestration	**7.1** Log All Traffic (Network, Data, Apps, Users)
1.2 Conditional User Access	**2.2** Device Detection and Compliance	**3.2** Secure Software Development & Integration	**4.2** DoD Enterprise Data Governance	**5.2** Software Defined Networking (SDN)	**6.2** Critical Process Automation	**7.2** Security Information and Event Management (SIEM)
1.3 Multi-Factor Authentication	**2.3** Device Authorization with Real Time Inspection	**3.3** Software Risk Management	**4.3** Data Labeling and Tagging	**5.3** Macro Segmentation	**6.3** Machine Learning	**7.3** Common Security and Risk Analytics
1.4 Privileged Access Management	**2.4** Remote Access	**3.4** Resource Authorization & Integration	**4.4** Data Monitoring and Sensing	**5.4** Micro Segmentation	**6.4** Artificial Intelligence	**7.4** User and Entity Behavior Analytics
1.5 Identity Federation & User Credentialing	**2.5** Partially & Fully Automated Asset, Vulnerability and Patch Management	**3.5** Continuous Monitoring and Ongoing Authorizations	**4.5** Data Encryption & Rights Management		**6.5** Security Orchestration, Automation & Response (SOAR)	**7.5** Threat Intelligence Integration
1.6 Behavioral, Contextual ID, and Biometrics	**2.6** Unified Endpoint Management (UEM) & Mobile Device Management (MDM)		**4.6** Data Loss Prevention (DLP)		**6.6** API Standardization	**7.6** Automated Dynamic Policies
1.7 Least Privileged Access	**2.7** Endpoint & Extended Detection & Response (EDR & XDR)		**4.7** Data Access Control		**6.7** Security Operations Center (SOC) & Incident Response (IR)	
1.8 Continuous Authentication						
1.9 Integrated ICAM Platform						

EXECUTION ENABLERS

- Doctrine
- Organization
- Training
- material
- Leadership & Education
- Personnel
- Facilities
- Policy

As of 09MAR2023

42 ZT *Capabilities* within TARGET + 3 ZT *Capabilities* within ADVANCED = 45 ZT *Capabilities* for Maximum Level ZT (full achievement of ADVANCED Level ZT within DoD)



Zero Trust Target Level

Advanced Zero Trust

Execution Enablers

Doctrine
Organization
Training
materiel
Leadership & Education
Personnel
Facilities
Policy

User

1.1 User Inventory

1.7 Least Privileged Access

1.2 Conditional User Access

1.3 Multifactor Authentication

1.4 Privileged Access Mgmt.

1.5 Identity Federation and User Credentialing

1.6 Behavioral, Contextual ID, & Biometrics

1.8 Continuous Authentication

1.9 Integrated ICAM Platform

Device

2.5 Partially & Fully Automated Asset, Vulnerability and Patch Mgmt.

2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM)

2.1 Device Inventory

2.2 Device Detection and Compliance

2.3 Device Authorization w/ Real Time Inspection

2.4 Remote Access

2.7 Endpoint & Extended Detection & Response (EDR & XDR)

Application & Workload

3.1 Application Inventory

3.3 Software Risk Management

3.2 Software Development & Integration

3.4 Resource Authorization & Integration

3.5 Continuous Monitoring and Ongoing Authorizations

Data

4.1 Data Catalog Risk Alignment

4.2 DoD Enterprise Data Governance

4.4 Data Monitoring & Sensing

4.3 Data Labeling & Tagging

4.5 Data Encryption & Rights Mgmt.

4.6 Data Loss Prevention

4.7 Data Access Control

Network & Environment

5.1 Data Flow Mapping

5.3 Macro Segmentation

5.2 Software Defined Networking

5.4 Micro Segmentation

Automation & Orchestration

6.3 Machine Learning

6.6 API Standardization

6.5 Security Orchestration, Automation, and Response

6.7 SOC & Incident Response

6.1 PDP & Orchestration

6.2 Critical Process Automation

6.4 Artificial Intelligence

Visibility & Analytics

7.1 Log All Traffic

7.3 Common Security & Risk Analytics

7.5 Threat Intelligence Integration

7.4 User & Entity Behavior Analytics (UEBA)

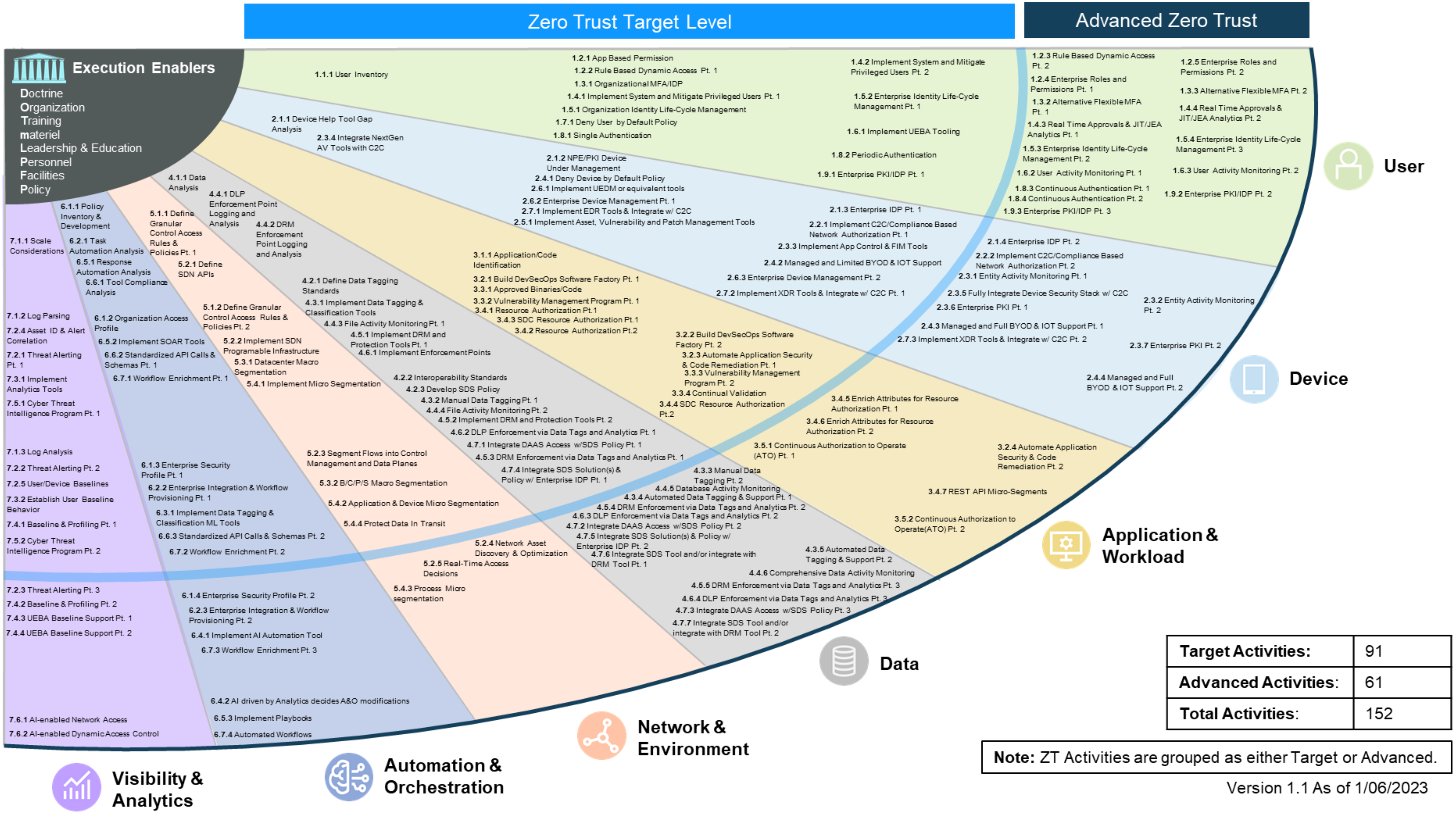
7.2 Security Information and Event Mgmt. (SIEM)

7.6 Automated Dynamic Policies

Note: ZT Capabilities in bold font and displayed on the ZT Target line contain activities spanning both Target and Advanced ZT.

V1.0 as of 10/04/2022

91 ZT *Activities* within TARGET + 61 ZT *Activities* within ADVANCED = 152 ZT *Activities* for Maximum Level ZT (full achievement of ADVANCED Level ZT within DoD)



Zero Trust Target Level

Advanced Zero Trust

Execution Enablers

Doctrine
Organization
Training
materiel
Leadership & Education
Personnel
Facilities
Policy

User

1.1.1 User Inventory
1.2.1 App Based Permission
1.2.2 Rule Based Dynamic Access Pt. 1
1.3.1 Organizational MFA/IDP
1.4.1 Implement System and Mitigate Privileged Users Pt. 1
1.5.1 Organization Identity Life-Cycle Management
1.7.1 Deny User by Default Policy
1.8.1 Single Authentication
1.4.2 Implement System and Mitigate Privileged Users Pt. 2
1.5.2 Enterprise Identity Life-Cycle Management Pt. 1
1.6.1 Implement UEBA Tooling
1.8.2 Periodic Authentication
1.9.1 Enterprise PKI/IDP Pt. 1
1.2.3 Rule Based Dynamic Access Pt. 2
1.2.4 Enterprise Roles and Permissions Pt. 1
1.3.2 Alternative Flexible MFA Pt. 1
1.4.3 Real Time Approvals & JIT/JEA Analytics Pt. 1
1.5.3 Enterprise Identity Life-Cycle Management Pt. 2
1.6.2 User Activity Monitoring Pt. 1
1.8.3 Continuous Authentication Pt. 1
1.8.4 Continuous Authentication Pt. 2
1.9.3 Enterprise PKI/IDP Pt. 3
1.2.5 Enterprise Roles and Permissions Pt. 2
1.3.3 Alternative Flexible MFA Pt. 2
1.4.4 Real Time Approvals & JIT/JEA Analytics Pt. 2
1.5.4 Enterprise Identity Life-Cycle Management Pt. 3
1.6.3 User Activity Monitoring Pt. 2
1.9.2 Enterprise PKI/IDP Pt. 2

Device

2.1.1 Device Help Tool Gap Analysis
2.3.4 Integrate NextGen AV Tools with C2C
2.1.2 NPE/PKI Device Under Management
2.4.1 Deny Device by Default Policy
2.6.1 Implement UEDM or equivalent tools
2.6.2 Enterprise Device Management Pt. 1
2.7.1 Implement EDR Tools & Integrate w/ C2C
2.5.1 Implement Asset, Vulnerability and Patch Management Tools
2.1.3 Enterprise IDP Pt. 1
2.2.1 Implement C2C/Compliance Based Network Authorization Pt. 1
2.3.3 Implement App Control & FIM Tools
2.4.2 Managed and Limited BYOD & IOT Support
2.6.3 Enterprise Device Management Pt. 2
2.7.2 Implement XDR Tools & Integrate w/ C2C Pt. 1
2.1.4 Enterprise IDP Pt. 2
2.2.2 Implement C2C/Compliance Based Network Authorization Pt. 2
2.3.1 Entity Activity Monitoring Pt. 1
2.3.5 Fully Integrate Device Security Stack w/ C2C
2.3.6 Enterprise PKI Pt. 1
2.4.3 Managed and Full BYOD & IOT Support Pt. 1
2.7.3 Implement XDR Tools & Integrate w/ C2C Pt. 2
2.3.2 Entity Activity Monitoring Pt. 2
2.3.7 Enterprise PKI Pt. 2
2.4.4 Managed and Full BYOD & IOT Support Pt. 2

Application & Workload

3.1.1 Application/Code Identification
3.2.1 Build DevSecOps Software Factory Pt. 1
3.3.1 Approved Binaries/Code
3.3.2 Vulnerability Management Program Pt. 1
3.4.1 Resource Authorization Pt.1
3.4.3 SDC Resource Authorization Pt.1
3.4.2 Resource Authorization Pt.2
3.2.2 Build DevSecOps Software Factory Pt. 2
3.2.3 Automate Application Security & Code Remediation Pt. 1
3.3.3 Vulnerability Management Program Pt. 2
3.3.4 Continual Validation
3.4.4 SDC Resource Authorization Pt.2
3.4.5 Enrich Attributes for Resource Authorization Pt. 1
3.4.6 Enrich Attributes for Resource Authorization Pt. 2
3.5.1 Continuous Authorization to Operate (ATO) Pt. 1
3.2.4 Automate Application Security & Code Remediation Pt. 2
3.4.7 REST API Micro-Segments
3.5.2 Continuous Authorization to Operate(ATO) Pt. 2

Data

4.1.1 Data Analysis
4.4.1 DLP Enforcement Point Logging and Analysis
4.4.2 DRM Enforcement Point Logging and Analysis
4.2.1 Define Data Tagging Standards
4.3.1 Implement Data Tagging & Classification Tools
4.4.3 File Activity Monitoring Pt. 1
4.5.1 Implement DRM and Protection Tools Pt. 1
4.6.1 Implement Enforcement Points
4.2.2 Interoperability Standards
4.2.3 Develop SDS Policy
4.3.2 Manual Data Tagging Pt. 1
4.4.4 File Activity Monitoring Pt. 2
4.5.2 Implement DRM and Protection Tools Pt. 2
4.6.2 DLP Enforcement via Data Tags and Analytics Pt. 1
4.7.1 Integrate DAAS Access w/SDS Policy Pt. 1
4.5.3 DRM Enforcement via Data Tags and Analytics Pt. 1
4.7.4 Integrate SDS Solution(s) & Policy w/ Enterprise IDP Pt. 1
4.3.3 Manual Data Tagging Pt. 2
4.4.5 Database Activity Monitoring
4.3.4 Automated Data Tagging & Support Pt. 1
4.5.4 DRM Enforcement via Data Tags and Analytics Pt. 2
4.6.3 DLP Enforcement via Data Tags and Analytics Pt. 2
4.7.2 Integrate DAAS Access w/SDS Policy Pt. 2
4.7.5 Integrate SDS Solution(s) & Policy w/ Enterprise IDP Pt. 2
4.7.6 Integrate SDS Tool and/or integrate with DRM Tool Pt. 1
4.3.5 Automated Data Tagging & Support Pt. 2
4.4.6 Comprehensive Data Activity Monitoring
4.5.5 DRM Enforcement via Data Tags and Analytics Pt. 3
4.6.4 DLP Enforcement via Data Tags and Analytics Pt. 3
4.7.3 Integrate DAAS Access w/SDS Policy Pt. 3
4.7.7 Integrate SDS Tool and/or integrate with DRM Tool Pt. 2

Network & Environment

5.1.1 Define Granular Control Access Rules & Policies Pt. 1
5.2.1 Define SDN APIs
5.1.2 Define Granular Control Access Rules & Policies Pt. 2
5.2.2 Implement SDN Programable Infrastructure
5.3.1 Datacenter Macro Segmentation
5.4.1 Implement Micro Segmentation
5.2.3 Segment Flows into Control Management and Data Planes
5.3.2 B/C/P/S Macro Segmentation
5.4.2 Application & Device Micro Segmentation
5.4.4 Protect Data In Transit
5.2.4 Network Asset Discovery & Optimization
5.2.5 Real-Time Access Decisions
5.4.3 Process Micro segmentation

Automation & Orchestration

6.1.1 Policy Inventory & Development
6.2.1 Task Automation Analysis
6.5.1 Response Automation Analysis
6.6.1 Tool Compliance Analysis
6.1.2 Organization Access Profile
6.5.2 Implement SOAR Tools
6.6.2 Standardized API Calls & Schemas Pt. 1
6.7.1 Workflow Enrichment Pt. 1
6.1.3 Enterprise Security Profile Pt. 1
6.2.2 Enterprise Integration & Workflow Provisioning Pt. 1
6.3.1 Implement Data Tagging & Classification ML Tools
6.6.3 Standardized API Calls & Schemas Pt. 2
6.7.2 Workflow Enrichment Pt. 2
6.1.4 Enterprise Security Profile Pt. 2
6.2.3 Enterprise Integration & Workflow Provisioning Pt. 2
6.4.1 Implement AI Automation Tool
6.7.3 Workflow Enrichment Pt. 3
6.4.2 AI driven by Analytics decides A&O modifications
6.5.3 Implement Playbooks
6.7.4 Automated Workflows

Visibility & Analytics

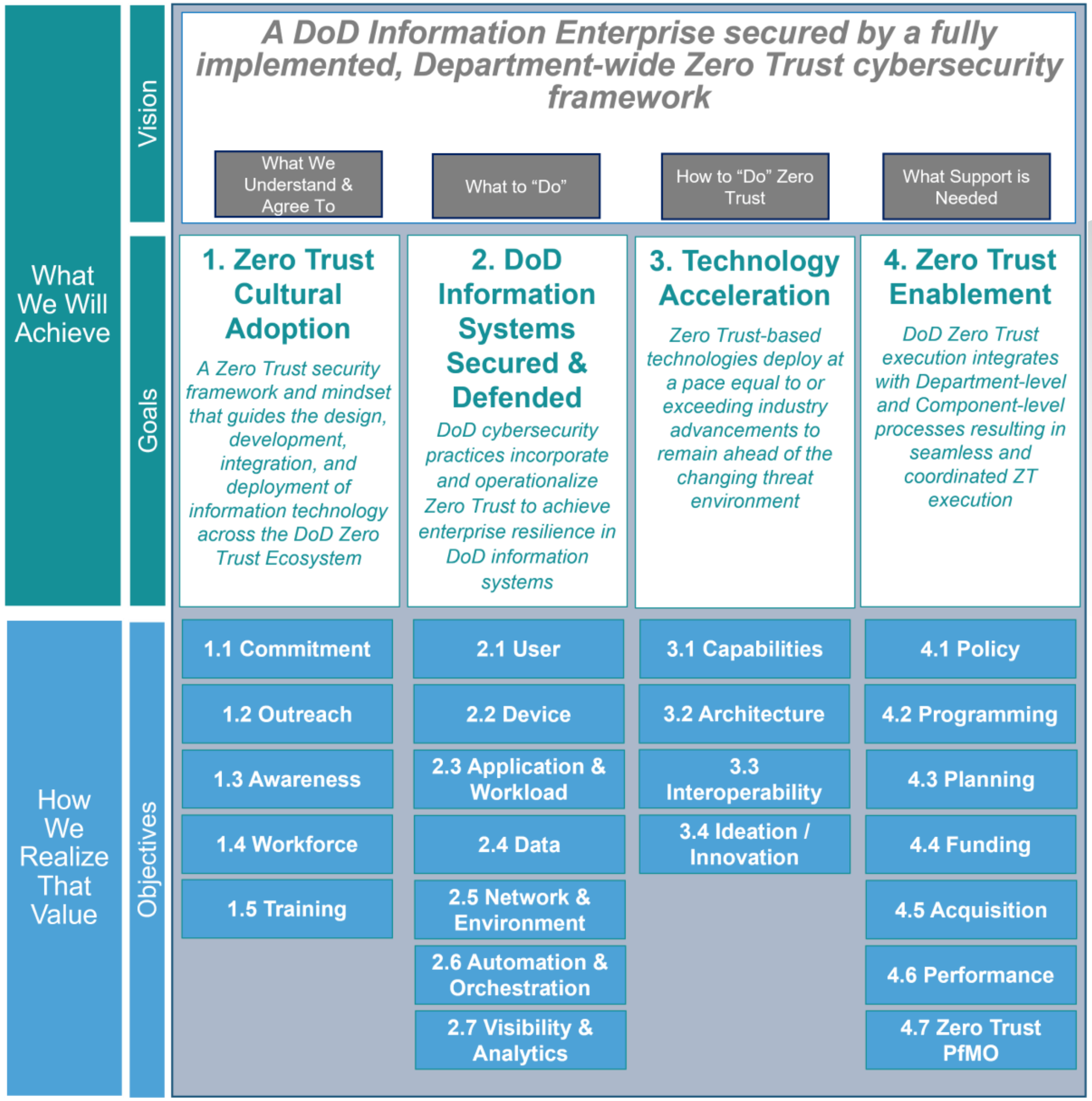
7.1.1 Scale Considerations
7.1.2 Log Parsing
7.2.4 Asset ID & Alert Correlation
7.2.1 Threat Alerting Pt. 1
7.3.1 Implement Analytics Tools
7.5.1 Cyber Threat Intelligence Program Pt. 1
7.1.3 Log Analysis
7.2.2 Threat Alerting Pt. 2
7.2.5 User/Device Baselines
7.3.2 Establish User Baseline Behavior
7.4.1 Baseline & Profiling Pt. 1
7.5.2 Cyber Threat Intelligence Program Pt. 2
7.2.3 Threat Alerting Pt. 3
7.4.2 Baseline & Profiling Pt. 2
7.4.3 UEBA Baseline Support Pt. 1
7.4.4 UEBA Baseline Support Pt. 2
7.6.1 AI-enabled Network Access
7.6.2 AI-enabled Dynamic Access Control

Target Activities:	91
Advanced Activities:	61
Total Activities:	152

Note: ZT Activities are grouped as either Target or Advanced.

Version 1.1 As of 1/06/2023

ZT Goals and Objectives to achieve ZT Target Level and Advance Target Level



What We Will Achieve

Vision

A DoD Information Enterprise secured by a fully implemented, Department-wide Zero Trust cybersecurity framework

What We Understand & Agree To	What to "Do"	How to "Do" Zero Trust	What Support is Needed

Goals

1. Zero Trust Cultural Adoption

A Zero Trust security framework and mindset that guides the design, development, integration, and deployment of information technology across the DoD Zero Trust Ecosystem

2. DoD Information Systems Secured & Defended

DoD cybersecurity practices incorporate and operationalize Zero Trust to achieve enterprise resilience in DoD information systems

3. Technology Acceleration

Zero Trust-based technologies deploy at a pace equal to or exceeding industry advancements to remain ahead of the changing threat environment

4. Zero Trust Enablement

DoD Zero Trust execution integrates with Department-level and Component-level processes resulting in seamless and coordinated ZT execution

How We Realize That Value

Objectives

1.1 Commitment	2.1 User	3.1 Capabilities	4.1 Policy
1.2 Outreach	2.2 Device	3.2 Architecture	4.2 Programming
1.3 Awareness	2.3 Application & Workload	3.3 Interoperability	4.3 Planning
1.4 Workforce	2.4 Data	3.4 Ideation / Innovation	4.4 Funding
1.5 Training	2.5 Network & Environment		4.5 Acquisition
	2.6 Automation & Orchestration		4.6 Performance
	2.7 Visibility & Analytics		4.7 Zero Trust PfMO

Zero Trust Cultural Adoption:

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

DoD Information Systems Secured and Defended:

- Secured communications at all operational levels
- Improved systems performance
- Interoperable & secured data
- Automated cyber and Artificial Intelligence (AI) operations

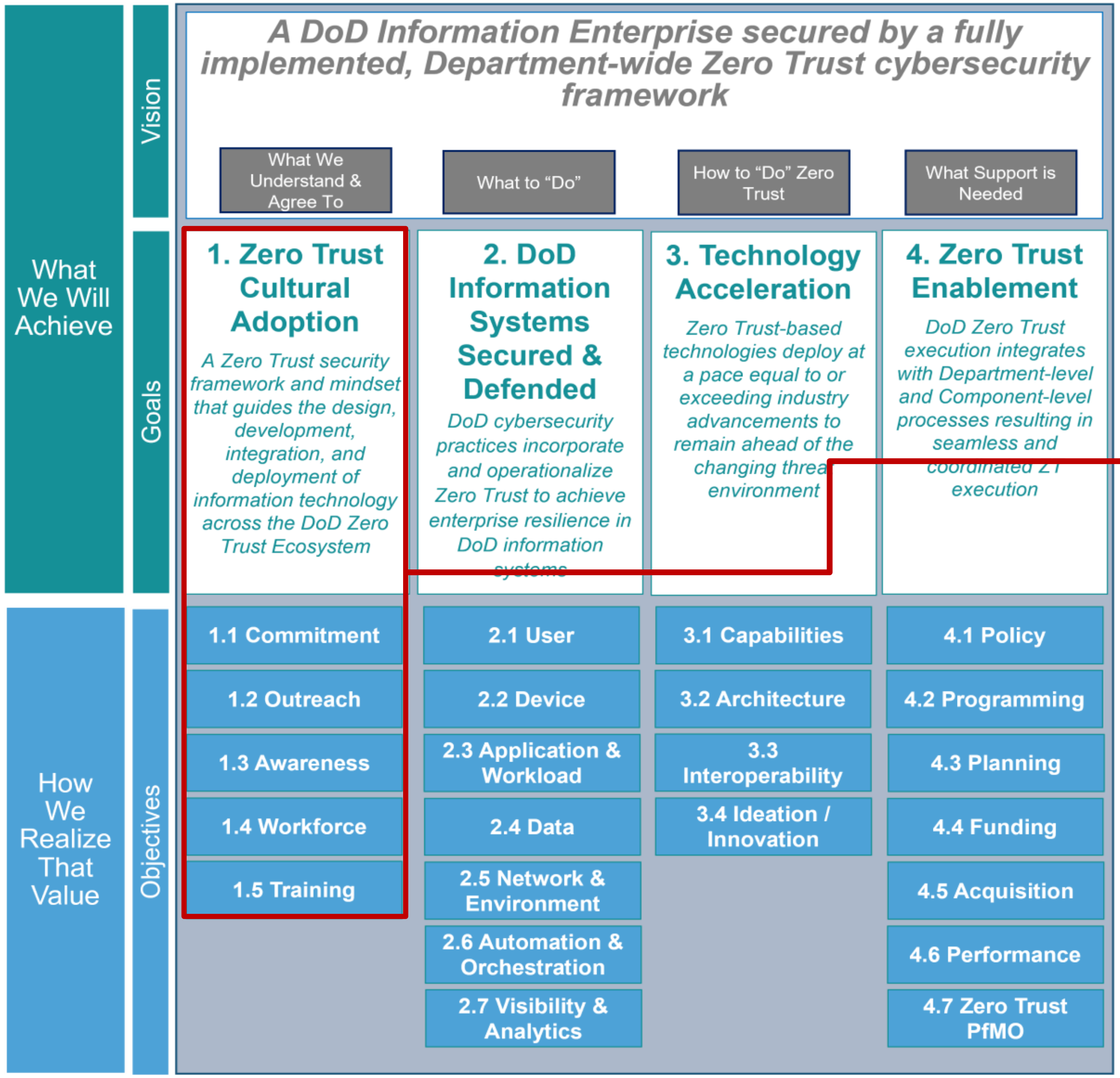
Technology Acceleration:

- Continually updated & advanced ZT enabled IT
- Reduced silos
- Simplified architecture
- Efficient data management

Zero Trust Enablement

- Enhanced operations and support performance
- Consistent, aligned, and effectively resourced ZT supporting functions
- Speed of ZT acquisition-to-deployed capability

How to Engage Us With Training and Drive Cultural Change



What We Will Achieve	Vision	*A DoD Information Enterprise secured by a fully implemented, Department-wide Zero Trust cybersecurity framework*			
		What We Understand & Agree To	What to "Do"	How to "Do" Zero Trust	What Support is Needed
	Goals	**1. Zero Trust Cultural Adoption** *A Zero Trust security framework and mindset that guides the design, development, integration, and deployment of information technology across the DoD Zero Trust Ecosystem*	**2. DoD Information Systems Secured & Defended** *DoD cybersecurity practices incorporate and operationalize Zero Trust to achieve enterprise resilience in DoD information systems*	**3. Technology Acceleration** *Zero Trust-based technologies deploy at a pace equal to or exceeding industry advancements to remain ahead of the changing threat environment*	**4. Zero Trust Enablement** *DoD Zero Trust execution integrates with Department-level and Component-level processes resulting in seamless and coordinated ZT execution*
How We Realize That Value	Objectives	1.1 Commitment	2.1 User	3.1 Capabilities	4.1 Policy
		1.2 Outreach	2.2 Device	3.2 Architecture	4.2 Programming
		1.3 Awareness	2.3 Application & Workload	3.3 Interoperability	4.3 Planning
		1.4 Workforce	2.4 Data	3.4 Ideation / Innovation	4.4 Funding
		1.5 Training	2.5 Network & Environment		4.5 Acquisition
			2.6 Automation & Orchestration		4.6 Performance
			2.7 Visibility & Analytics		4.7 Zero Trust PfMO

Zero Trust Cultural Adoption

"How The Department protects and secures the DoD IE is not solvable by technology alone; it requires a change in mindset and culture, from DoD leadership down to mission operators, spanning all users of the DoD IE."

- *DoD Zero Trust Strategy*, 21 Oct 2022

DoD ZT Implementation Course of Actions

Under Testing between 3Q-4Q FY23

COA 1

and/or

COA 2

and/or

COA 3

ZT Baseline

- Leverages current infrastructure and environment using Brownfield approach
- Zero Trust "on the ground" modernization: ~ 5^{+} yr. (FYDP beginning FY23) Implementation Plan
- Establishes set capabilities and activities needed to achieve Target and Advanced-levels of Zero Trust
- No constraints on tools or methods to accomplish ZT

Commercial Cloud

- Relies on commercial provider(s) to develop ZT compliant cloud environments using Greenfield approach
- Achieves DoD ZT quicker than COA-1
- Mandate would be to achieve DoD ZT "Target" level, at a minimum
- Provides standardized tools and capabilities to support ZT execution

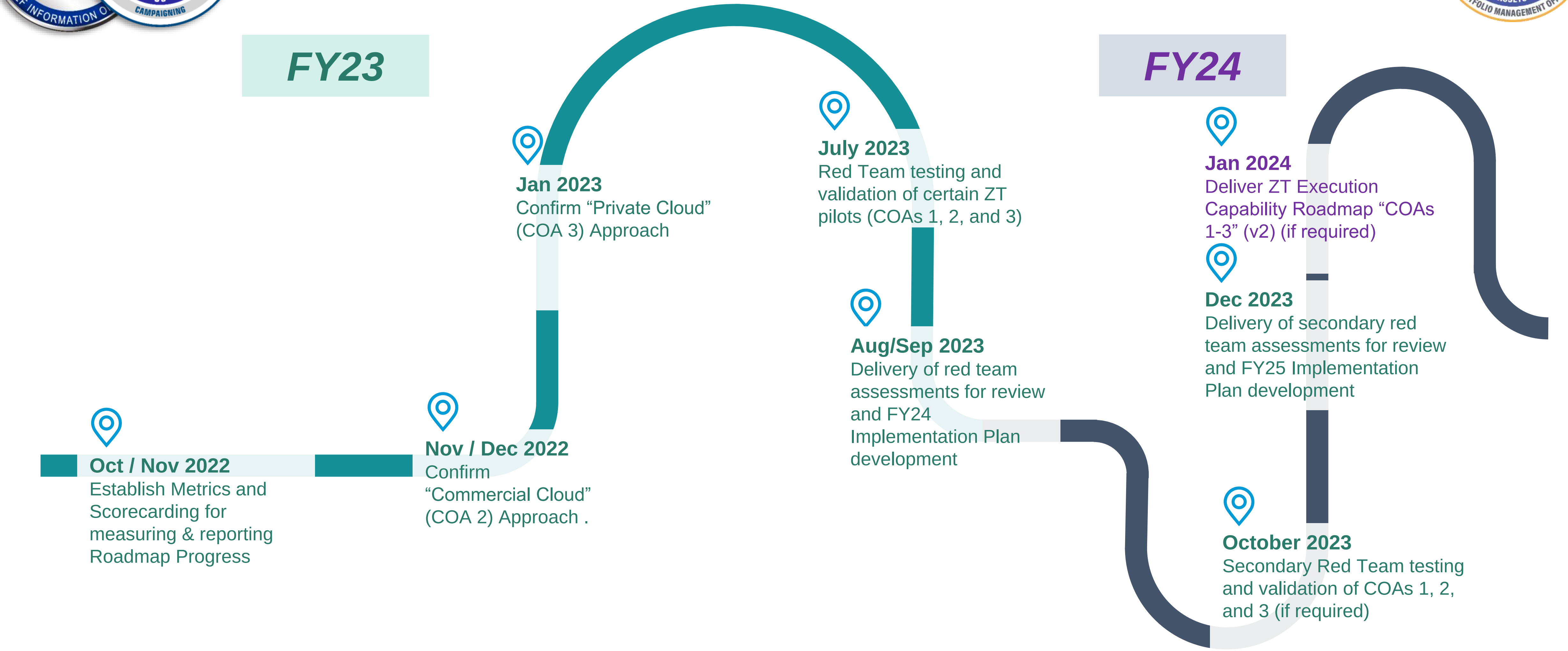
Private Cloud

- Government Owned/Operated high-performance Native ZT Cloud (NZTC) using Greenfield approach
- Achieves DoD ZT quicker than COA-1
- Achieves immediate DoD ZT "Advanced" level by design, which needs to be independently validated
- Three possible ZT Cloud sizing options being considered for DoDIN:
  1) Enterprise compute and storage
  2) Edge compute and storage
  3) Tactical compute and storage

COA-2 and COA-3 Activities

- RFI to CSPs on ability to meet Target and/or Advanced Level ZT- August 2022
  - Microsoft, Amazon, Oracle, Google, and IBM
  - Pilots to be conducted this Summer/Fall 2023 to test assertions of CSP’s
- Testing
  - Engaging with DOT&E to Red Team
    - Testing planned for July 2023, possibly in two phases, July then again in October 2023:
      - Amazon - USAF
      - Google - USA
      - IBM – ODNI
      - Microsoft - USN, Cloud 42
      - Oracle - DMDC
  - Leveraging ATT&CK mapping and Control analysis for CSP ZT test plans & Red Teams
- COA-3: (note: must meet Target Level ZT by end of FY27)
  - SABRE/MPE (Advanced Level ZT)
  - Other MPE’s (Target Level ZT?)
  - Non-CSP vendors are showing interest in building COA-3 ZT solutions @ Advanced Level based on NZTC design. Multiple configurations mentioned – Data Center level, Base level, Tactical Edge level/DDIL/disconnected.

COA-2 & COA-3 Schedule



FY23

Oct / Nov 2022
Establish Metrics and Scorecarding for measuring & reporting Roadmap Progress

Nov / Dec 2022
Confirm "Commercial Cloud" (COA 2) Approach .

Jan 2023
Confirm "Private Cloud" (COA 3) Approach

July 2023
Red Team testing and validation of certain ZT pilots (COAs 1, 2, and 3)

Aug/Sep 2023
Delivery of red team assessments for review and FY24 Implementation Plan development

FY24

October 2023
Secondary Red Team testing and validation of COAs 1, 2, and 3 (if required)

Dec 2023
Delivery of secondary red team assessments for review and FY25 Implementation Plan development

Jan 2024
Deliver ZT Execution Capability Roadmap "COAs 1-3" (v2) (if required)

Zero Trust Training Levels and Vision

Training	Level 1	Level 2	Level 3
Definition of Training Level	• Basic Awareness for the Entire DoD (Light technical)	• Training for IT, Engineers, and others with interest beyond Awareness (Moderate Technical)	• Training for Practitioners and Implementers • Chief Engineers & Architects, IT Implementers (Moderate to heavy technical)
Personnel to train (5 years, est.)	4,000,000	200,000	40,000
How training can be accomplished	Online training and Conferences and Symposiums	Online Training, webinars, Conferences and Symposiums	Workshops (Virtual Instructor led training and on location)
Training Plan	• ZT Awareness & ZT Executive course via Joint Knowledge Online (JKO) portal, • DoD ZT Symposium (annual)	• ZT Implementation & Policy/ Guidance course via JKO, • DoD ZT Symposium (annual)	• ZT Practitioners Workshop (Virtual & on location, monthly) • Chief Engineer Workshop (On-location, quarterly)
Challenges	• Requires leadership buy-in	• Depth of training • Effectiveness for online only	• Cannot train all practitioners • Level 3 must train the trainer

https://www.dau.edu/News/Zero-Trust-Training-for-the-DoD-Community

Major Zero Trust Training Events

Details	Virtual DoD Zero Trust Symposium	DoD Chief Engineers’ Workshop (Laurel, MD)
Capacity per event	5,000	200
Date/ Frequency	4-5 April, 2023/ Yearly	20-21 June, 2023/ Quarterly in FY 24
Target Audience	DoD, Academia & Industry interested in ZT	DoD & Industry Chief Engineers & Architects that Implement ZT
Host/ Delivery Method	MIT/ Zoomgov Webinar (all virtual)	Johns Hopkins, Laurel, MD Campus
Purpose	Demonstrate need & value of ZT via academic & industry research, case studies, and DoD presentations. Promote cultural change	Apply & evaluate ZT solutions for implementing ZT via COA 1, 2 &3
Desired outcomes	- Leaders better understand need for ZT & effective ZT implementation (Cultural change) - Increased collaboration among Academia, Industry & Government	- Greater discernment for Effective ZT Implementation - Ability to apply ZT implementation lessons learned
Key Participants	DAU, MIT, CIO, JHU, CSA, DoD, John Kindervag	DAU, JHU, CIO, Carnegie Mellon, DoD
Summary	*“How The Department protects and secures the DoD IE is not solvable by technology alone; it requires a change in mindset and culture…”* DoD Zero Trust Strategy, 11/22/2022	*“A workshop with engineers and architects to get everyone to understand the basic concepts of ZT and build a prototype implementation is usually our starting point.”* Rob Maas, ZT SME

DoD Zero Trust Strategy Timeline

As of 25 April 2023

● Milestone Due

◆ Milestone Event

Milestone Process

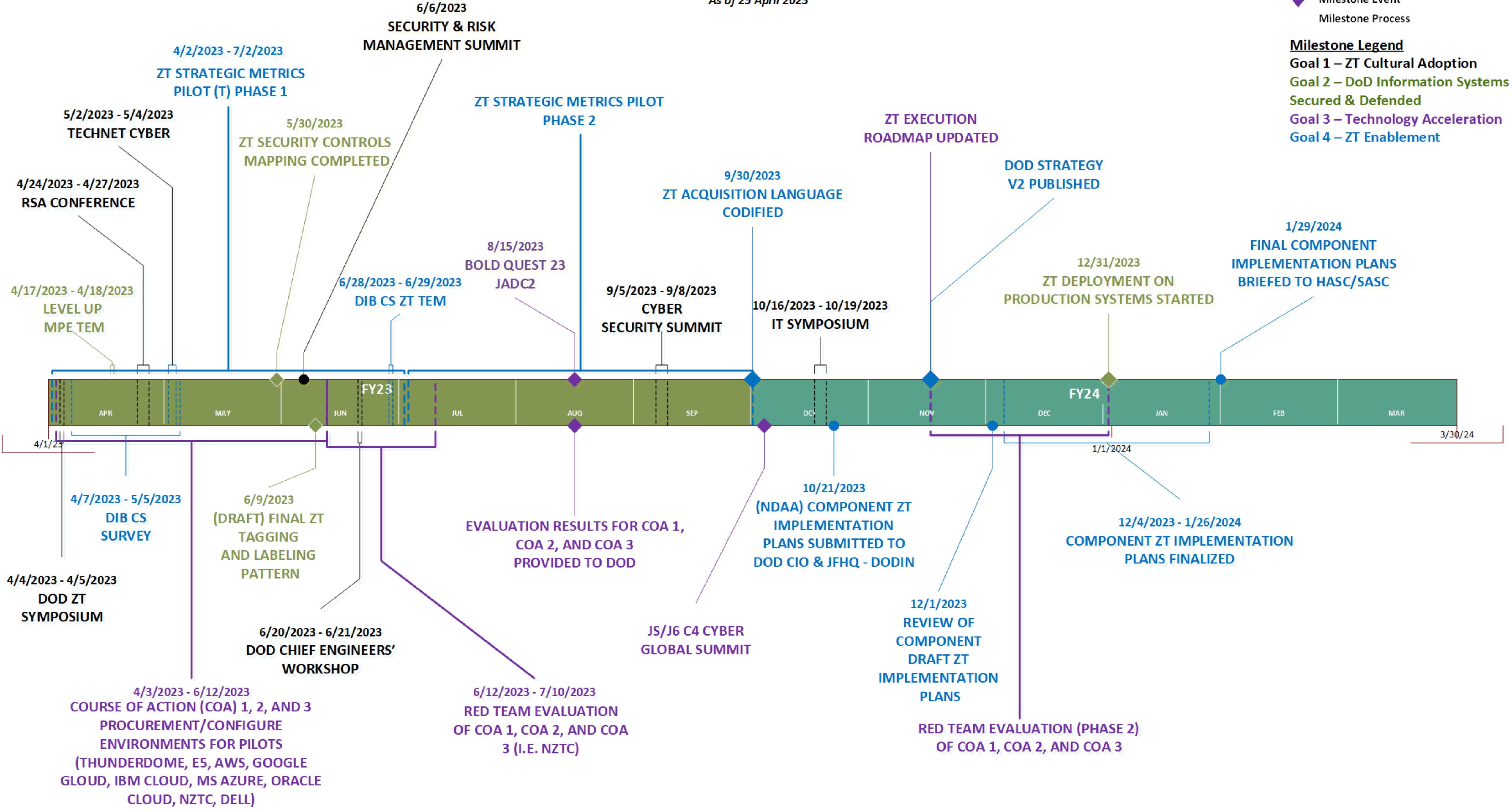
Milestone Legend

Goal 1 – ZT Cultural Adoption

Goal 2 – DoD Information Systems Secured & Defended

Goal 3 – Technology Acceleration

Goal 4 – ZT Enablement



4/17/2023 - 4/18/2023
LEVEL UP
MPE TEM

4/24/2023 - 4/27/2023
RSA CONFERENCE

5/2/2023 - 5/4/2023
TECHNET CYBER

4/2/2023 - 7/2/2023
ZT STRATEGIC METRICS
PILOT (T) PHASE 1

5/30/2023
ZT SECURITY CONTROLS
MAPPING COMPLETED

6/6/2023
SECURITY & RISK
MANAGEMENT SUMMIT

6/28/2023 - 6/29/2023
DIB CS ZT TEM

ZT STRATEGIC METRICS PILOT
PHASE 2

8/15/2023
BOLD QUEST 23
JADC2

9/5/2023 - 9/8/2023
CYBER
SECURITY SUMMIT

9/30/2023
ZT ACQUISITION LANGUAGE
CODIFIED

10/16/2023 - 10/19/2023
IT SYMPOSIUM

ZT EXECUTION
ROADMAP UPDATED

DOD STRATEGY
V2 PUBLISHED

12/31/2023
ZT DEPLOYMENT ON
PRODUCTION SYSTEMS STARTED

1/29/2024
FINAL COMPONENT
IMPLEMENTATION PLANS
BRIEFED TO HASC/SASC

4/4/2023 - 4/5/2023
DOD ZT
SYMPOSIUM

4/7/2023 - 5/5/2023
DIB CS
SURVEY

6/9/2023
(DRAFT) FINAL ZT
TAGGING
AND LABELING
PATTERN

4/3/2023 - 6/12/2023
COURSE OF ACTION (COA) 1, 2, AND 3
PROCUREMENT/CONFIGURE
ENVIRONMENTS FOR PILOTS
(THUNDERDOME, E5, AWS, GOOGLE
GLOUD, IBM CLOUD, MS AZURE, ORACLE
CLOUD, NZTC, DELL)

6/20/2023 - 6/21/2023
DOD CHIEF ENGINEERS'
WORKSHOP

6/12/2023 - 7/10/2023
RED TEAM EVALUATION
OF COA 1, COA 2, AND COA
3 (I.E. NZTC)

EVALUATION RESULTS FOR COA 1,
COA 2, AND COA 3
PROVIDED TO DOD

JS/J6 C4 CYBER
GLOBAL SUMMIT

10/21/2023
(NDAA) COMPONENT ZT
IMPLEMENTATION
PLANS SUBMITTED TO
DOD CIO & JFHQ - DODIN

12/1/2023
REVIEW OF
COMPONENT
DRAFT ZT
IMPLEMENTATION
PLANS

RED TEAM EVALUATION (PHASE 2)
OF COA 1, COA 2, AND COA 3

12/4/2023 - 1/26/2024
COMPONENT ZT IMPLEMENTATION
PLANS FINALIZED

Col Gary R. Kipe

Deputy Director, DoD Zero Trust Portfolio Management Office
DoD CIO/CS
The Pentagon, Room 3D1048
Email: gary.r.kipe.mil@mail.mil
Ph: (703) 614-2999

Questions?

General ZT PfMO Mailbox:

osd.pentagon.dod-cio.mbx.dcio-cs-zt@mail.mil
tammy.a.bean2.civ@mail.mil
harmanpaul.s.brar.ctr@mail.mil