DoD Zero Trust Strategy

October 21, 2022

Prepared by: ZT PfMO

Change History

Version	Date	Page(s) Changed	Comments
1.0	10/21/2022		Initial published version

Foreword

Our adversaries are in our networks, exfiltrating our data, and exploiting the Department's users. The rapid growth of these offensive threats emphasizes the need for the Department of Defense (DoD) to adapt and significantly improve our deterrence strategies and cybersecurity implementations. Defending DoD networks with high-powered and ever-more sophisticated perimeter defenses is no longer sufficient for achieving cyber resiliency and securing our information enterprise that spans geographic borders, interfaces with external partners, and support to millions of authorized users, many of which now require access to DoD networks outside traditional boundaries, such as work from home. To meet these challenges, the DoD requires an enhanced cybersecurity framework built upon Zero Trust principles that must be adopted across the Department, enterprise-wide, as quickly as possible as described within this document.

This urgency means that our colleagues, our warfighters, and every member of DoD must adopt a Zero Trust mindset, regardless of whether they work in technology or cybersecurity or the Human Resource department. This "never trust, always verify" mindset requires us to take responsibility for the security of our devices, applications, assets, and services; users are granted access to only the data they need and when needed. We all must play a role in combating our adversaries by acting quickly and correctly to address security threats wherever and whenever they arise.

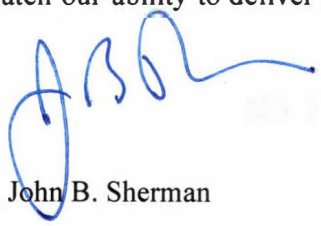
Zero Trust is much more than an IT solution. Zero Trust may include certain products but is not a capability or device that may be bought. The journey to Zero Trust requires all DoD Components to adopt and integrate Zero Trust capabilities, technologies, solutions, and processes across their architectures, systems, and within their budget and execution plans. Perhaps most importantly, they must also address Zero Trust requirements within their staffing, training, and professional development processes as well.

This Zero Trust strategy, the first of its kind for the Department, provides the necessary guidance for advancing Zero Trust concept development; gap analysis, requirements development, implementation, execution decision-making, and ultimately procurement and deployment of required ZT capabilities and activities which will have meaningful and measurable cybersecurity impacts upon adversaries. Importantly, this document serves only as a strategy, not a solution architecture. Zero Trust Solution Architectures can and should be designed and guided by the details found within this document.

In January 2022, the Department established the DoD Zero Trust Portfolio Management Office (ZT PfMO) within the DoD CIO, to orchestrate the DoD efforts outlined in this *DoD Zero Trust Strategy* document and to accelerate ZT adoption through several courses of action. Recognizing that the starting point for Zero Trust and maturity levels varies between components, Components

must align their ZT solution architectures and execution plans accordingly to this strategy so that overall DoD Enterprise ZT outcomes are achieved and in alignment to the DoD ZT PfMO schedule.

We must adapt, remain agile, and execute on synchronizing Zero Trust efforts across and throughout the Department. If we do not do this together, our teammates' vulnerabilities will remain exposed and open to attack, which makes all of us less strong. We need to make certain that when malicious actors attempt to breach our Zero Trust defenses; they can no longer roam freely through our networks and threaten our ability to deliver maximum support to the warfighter.



John B. Sherman

Executive Summary

"Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life."

— Executive Order on Improving the Nation's Cybersecurity 12 May 2021

Five Years into the Future

The Department of Defense's (DoD) risk-based Zero Trust Framework employed across the Joint Force and the defense ecosystem protects our information systems[1] from increasingly sophisticated attacks as our adversaries seek to affect our warfighters and DoD mission success. Zero Trust principles are now integrated into each of the five cybersecurity functions that represent key elements of a successful and holistic cybersecurity program – Identify, Protect, Detect, Respond, and Recover.[2] As a result, DoD will successfully mitigate attempts to deny, degrade, disrupt, deceive, or destroy our information systems. Operators at all levels are confident that the data accessed, the assets deployed, the applications used, and the services provided are secured and resilient.

Today

The Department's Information Enterprise is under wide scale and persistent attack from known and unknown malicious actors. The Department's most consequential strategic competitor and the pacing challenge for the Department, the People's Republic of China,[3] as well as other state-sponsored adversaries and individual malicious actors often breach the Department's defensive perimeter and roam freely within our information systems. The Department must act now.

Vulnerabilities exposed by data breaches inside and outside the Department of Defense demonstrate the need for a new, more robust cybersecurity framework that facilitates well-informed risk-based decisions.[4] Zero Trust security eliminates the traditional idea of perimeters, trusted networks, devices, personas, or processes and shifts to multi-attribute-based levels of confidence that enable authentication and authorization policies founded on the concept of least privileged access. Implementing the Zero Trust Framework requires designing a more efficient architecture that enhances security, the user experience, and overall mission performance.

Zero Trust uses continuous multi-factor authentication, micro-segmentation, advanced encryption, endpoint security, analytics, and robust auditing, among other capabilities, to fortify data,

---

[1] Information system includes "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information". See DoD Instruction (DoDI) 5000.82, *Acquisition of Information Technology (IT)*, 21 Apr 2020, p. 17.

[2] See US National Institute of Standards and Technology (NIST), Special Publication 1271, *Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide*, 6 August 2021, for descriptions of cybersecurity core functions and a set of guidelines for mitigating organizational cybersecurity risks.

[3] *Fact Sheet: 2022 National Defense Strategy*, 28 March 2022.

[4]Risk" refers to probability of an undesired event or condition and 2) the consequences, impact, or severity of the undesired event, were it to occur. See *DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs,* January 2017, p. 3

applications, assets, and services to deliver cyber resiliency. The Department is evolving to become a more agile, more mobile, cloud-supported workforce, collaborating with the entirety of DoD enterprise, including federal and non-federal organizations and mission partners working on a variety of missions. The Zero Trust Framework will reduce the attack surface, reduce risk, offer opportunities to manage the full range of risks (e.g., policy, programming, budgeting, execution, cybersecurity-specific, and others) and enable more effective data-sharing in partnership environments. It will also ensure that any adversary damage is quickly contained and remediated if a device, network, user, or credential is compromised.

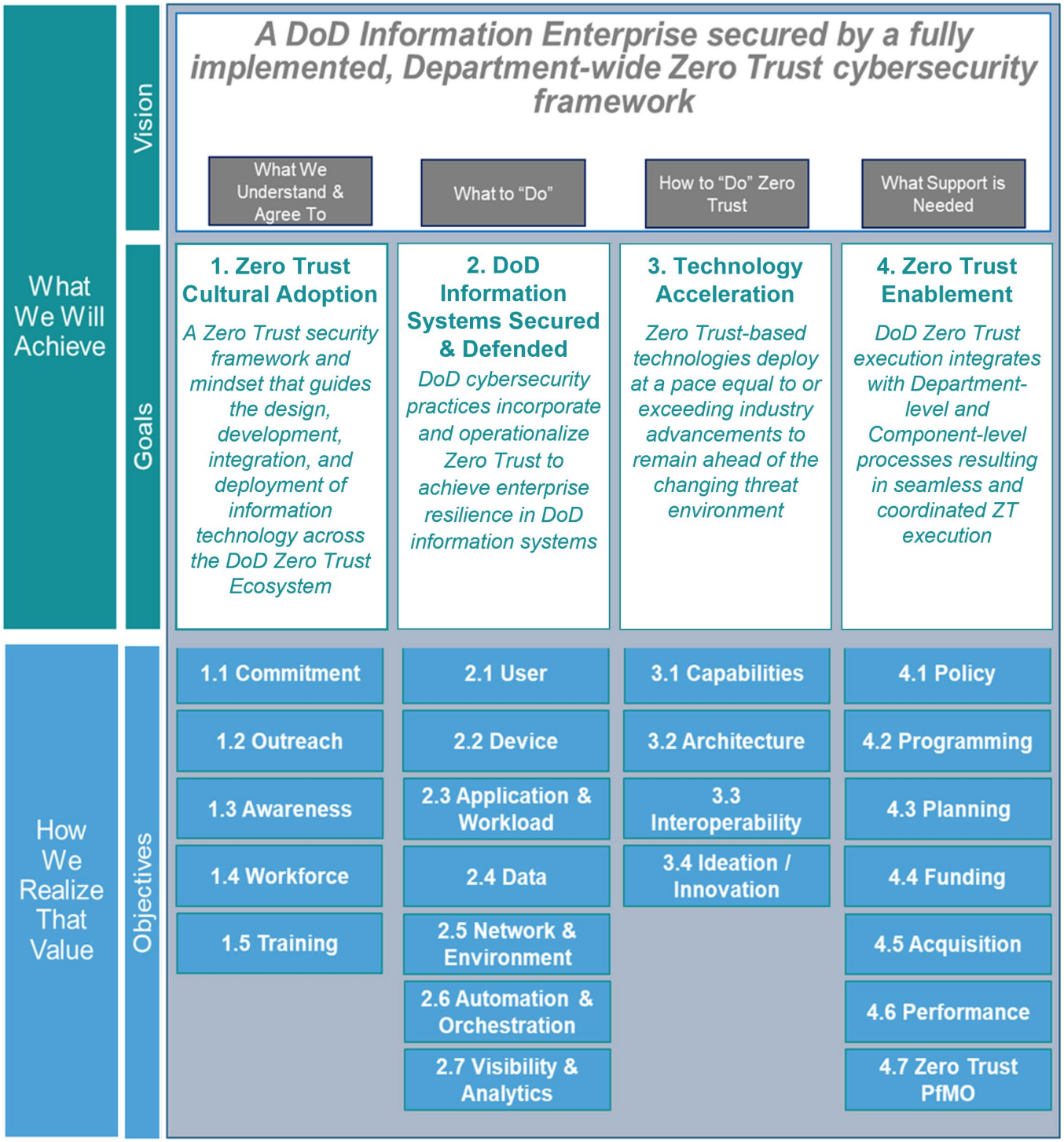
This strategy lays out the Department's vision for Zero Trust and sets a path to achieve it. It includes the strategic assumptions and principles that will inform and guide the adoption of ZT and the strategic goals and objectives. The *four strategic goals* outlined in this strategy are: 1. *Zero Trust Culture Adoption*, 2. *DoD Information Systems Secured and Defended*, 3. *Technology Acceleration*, and 4. *Zero Trust Enablement*. The strategy also refers to the seven DoD Zero Trust Pillars, which is the basis for the strategy's *Zero Trust Capability Roadmap*, a capabilities-based execution plan, and the DoD Zero Trust and Cybersecurity Reference Architectures. Finally, this strategy provides high-level guidance on resourcing and acquisition, measurement and metrics, and governance. The appendices include strategic and execution milestones, as well as references and definitions.

To accelerate Zero Trust implementation within the DoD Information Enterprise, the Department must continue to examine how to streamline and enforce resource priorities to meet the requirements envisioned by this strategy. In January 2022, the DoD CIO established a Zero Trust Portfolio Management Office (PfMO) to orchestrate DoD-wide Zero Trust execution, simplify and streamline existing policies and coordinate the prioritization of resources to accelerate Zero Trust adoption within the DODIN enterprise.

Figure 1 below depicts a concise view of the vision, goals, and objectives the Department will achieve by implementing the strategy.[5]

[5] See **Figure 4** in this document for an outcome description of each goal and objective.

Figure 1. DoD Zero Trust Strategy-at-a-Glance



Contents

Introduction

This Zero Trust Strategy defines an adaptive approach for how DoD must champion and accelerate the shift to a Zero Trust architecture and framework that secures and protects DoD Information Enterprise (IE)[6] within the Joint Information Environment (JIE)[7] and specifically the DoD Information Network (DODIN).[8] The intent of the strategy is to establish the parameters and target levels necessary to achieve Zero Trust (ZT) adoption across systems and networks (e.g., Non-classified Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet)). This approach emphasizes the need for DoD and its Components[9] to embrace evolving technology while adapting and responding to known and unknown malicious actors. It involves the full breadth of stakeholders in the DoD ZT Ecosystem[10] and allows strategic implementation to begin immediately.

Zero Trust is the term for an "*evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources*."[11] At its core, ZT assumes no implicit trust is granted to assets or users based solely on their physical or network location (i.e., local area networks versus the Internet) or asset ownership (enterprise or personally owned).[12] This shift in philosophy is a significant change in legacy authentication and security mechanisms. It also represents a major cultural change that stakeholders throughout the DoD ZT Ecosystem, including the Defense Industrial Base (DIB), will need to embrace and execute beginning with FY2023 through FY2027 and in the future.

---

[6] DoD Directive (DoDD) 8000.01, Chg 1; *Management of the Department of Defense Information Enterprise (DoD IE)*, Section 3(d), 17 July 2017, defines the DoD IE to include: "the DoD information network infrastructure, DoD enterprise IT service and solutions, National Security Systems, Industrial Control Systems, and embedded computing of wired, wireless, mobile communication, and platforms."

[7] *DoD Digital Modernization Strategy*, 5 June 2019, pp. 35 -36 defines the Joint Information Environment (JIE) as "a framework comprising a set of discrete initiatives developed and delivered as funded to support continual, comprehensive Department-wide IT Modernization and advance DoD information superiority in a common, coordinated way." It also notes "the JIE also includes deployed tactical components that are designed to work with core infrastructure and also operate autonomously, should connectivity to the core JIE be lost or denied."

[8] *Joint Publication 6-0 Joint Communications System*, 10 June 2015, Incorporating Change 1, 04 October 2019, defines DODIN as "The set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone."

[9] IBID defines DoD Components as the Office of the Secretary of Defense, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within DoD.

[10] See Appendix F for definition of DoD ZT Ecosystem, which consists of the breadth of DoD leaders, mission owners, and partners (internal and external) who are key stakeholders to successfully implement Zero Trust across the Information Enterprise (IE).

[11] The DoD defines Zero Trust in accordance with NIST SP 800-207, *Zero Trust Architecture*, August 2020, p. ii.

[12] IBID.

This strategy also highlights DoD CIO-led efforts, through the ZT Portfolio Management Office (PfMO), to accelerate ZT as part of its responsibilities for all matters relating to the DoD IE:[13] 1) Component information network infrastructure; 2) DoD enterprise IT service and solutions; 3) National Security Systems;[14] 4) Industrial Control Systems; 5) and embedded computing of wired, wireless, mobile communication, and platforms.[15]

Strategic Context

Warfighter missions demand secure, interoperable information systems. The intended outcomes and actions of the DoD ZT Framework[16] must support and enhance warfighter mission-critical priorities at all levels of the Department and align with the *DoD National Defense Strategy*. These outcomes and actions must be applied across all military multi-domain operations (cyber, space, air, ground, and sea) and supporting business assets. As coalition warfare becomes increasingly prevalent, interoperability of the DoD IE, with coalition networks,

Trusted Interoperability Data for Warfighters

Military targeteers need secure access to data at the speed of relevance they can use and trust. Warfighters need to target the right adversaries, accurately, while minimizing civilian and other casualties. Today, DoD data is often siloed, in impractical formats, and not fully vetted or secured from point of origin to use. The execution of Zero Trust provides targeteers trusted, tagged, and labeled data so they can confidently employ and share it with trusted partners, assured that the data is protected, secure, and accessed by only the people who need it, when they need it, using least privilege principles.

[13] DoDD 5144.02, Chg 1: *DoD Chief Information Officer*, Section 3, 19 September 2017, notes "The DoD CIO is responsible for all matters relating to the DoD information enterprise, including communications; spectrum management; network policy and standards; information systems; cybersecurity; positioning, navigation, and timing (PNT) policy; and the DoD information enterprise that supports DoD command and control (C2)."

[14] Although applicable to all the DoD, including Components that own and operate National Security Systems (NSS), this Strategy does not impact the authority and responsibilities of the Director of the National Security Agency (NSA) in connection with the National Manager responsibilities for NSS assigned to the Director of the NSA by National Security Directive 42 (NSD-42), *National Policy for the Security of National Security Telecommunications and Information Systems*, 5 July 1990. The NSS National Manager rather than the DoD sets NSS Zero Trust guidance.

[15] DoDD 8000.01, Chg 1; *Management of the Department of Defense Information Enterprise (DoD IE)*, Section 3(d), 17 July 2017, directs that all aspects of the IE "will be planned, designed, developed, architected, configured, acquired, managed, operated, and protected in order to help achieve an information advantage and full spectrum superiority, deliver mission assurance, improve mission effectiveness, and realize IT efficiencies." Available at

[16] For purposes of this *Strategy*, the DoD ZT Framework is defined as "an official cybersecurity blueprint, based on the seven DoD Zero Trust Capability Pillars, which describes how the Department will achieve ZT by providing the foundation and the direction to help align on-going and future ZT-related efforts, investments and initiatives". See

is critical.[17] ZT enables information dominance across the communications spectrum in the tactical environment by ensuring the security of data, applications, assets and services (DAAS). Execution plans must account for the potential ramifications of ZT in the tactical environment.

Mission impacts and vulnerabilities exposed by breaches and threats from inside and outside DoD and its Components, near-peer adversaries, geopolitical changes, and disruptive events, such as the global COVID pandemic, increase cybersecurity risks and the need for more resilient, scalable, and multi-disciplinary cybersecurity defense.

DoD's migration to increased remote work, an unprecedented technology refresh while divesting outdated technologies, shifts to artificial intelligence and cloud-based technologies complicate these trends. Advances in technology amplify the means to exfiltrate sensitive data from DoD and National Security Systems (NSS) and allow malicious actors the potential to inflict serious damage to DoD's information environment. These factors, combined with the expansion of partner relationships, create opportunities for malicious actors, using limited technical resources, to impact national security.

Cyber threats and attacks are evolving at an ever-increasing pace and requiring a coordinated, defensive response that is adaptive, flexible, and agile.[18] Traditional perimeter or "castle-and-moat" security approaches based on conventional authentication and authorization models do not work effectively to thwart current (and future) cyber-attack vectors. Mission and system owners, as well as operators, increasingly embrace this view as fact. They also see the journey to ZT as an opportunity to affect positively the mission by addressing technology modernizations, refining security processes, and improving operational performance.

Recognizing the need to address these cybersecurity challenges, the U.S. Federal Government is moving to a Zero Trust Architecture.[19] The *DoD Zero Trust Strategy* aligns with and responds to this Executive-level guidance for the Department. For example, the *Executive Order on Improving the Nation's Cybersecurity (EO 14028)* (12 May 2021), the N*ational Defense Authorization Act for Fiscal Year 2022* (27 December 2021), the *Federal Zero Trust Architecture Strategy* (26 Jan 2022), *National Security Memorandum-8, Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems* (19 January 2022), and numerous memoranda from the NSS National Manager directing all NSS's move to Zero Trust and act now.[20]

Appendix F.

[17] Mission partner environment (MPE) initiatives and secret and below releasable environment (SABRE) software seek to achieve network interoperability with coalition partners. See "Mission Partner Environment Cuts Decision Making, Kill Chain," DoD News, 29 November 2021.

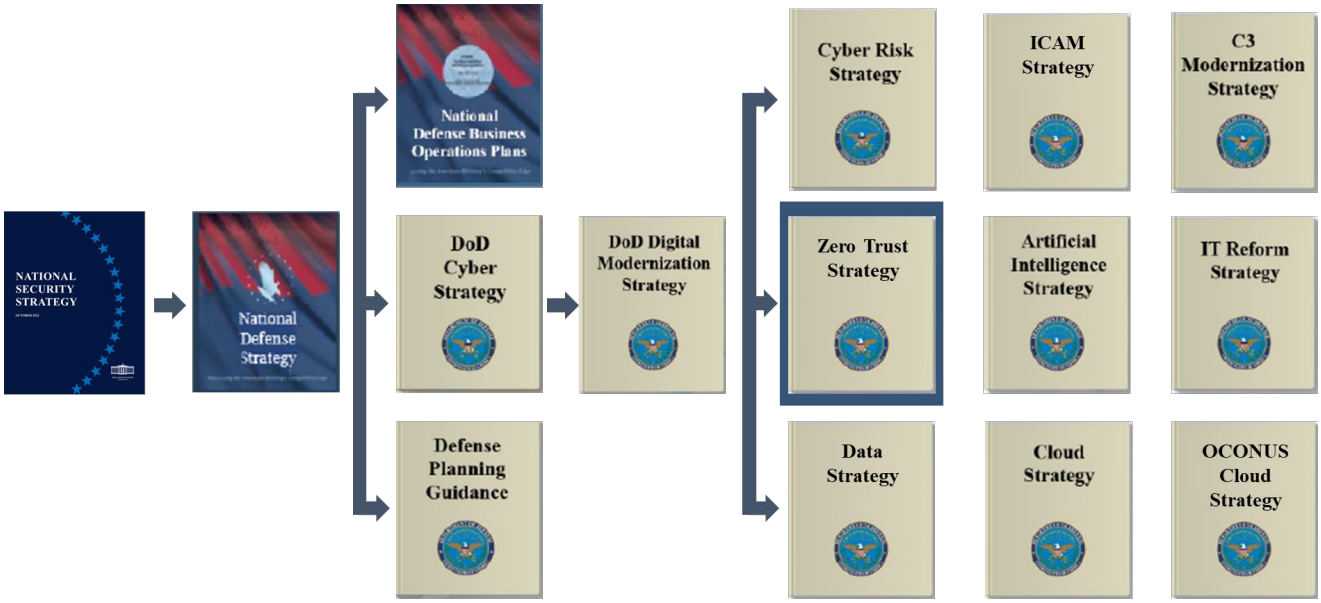
[18] See the classified 2018 *DoD Cyber Strategy* for further details on the strategic environment.

[19] *Office of Management and Budget (OMB) Memorandum M-22-09*,"Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," 26 January 2022.

[20] *Executive Order on Improving the Nation's Cybersecurity (EO 14028)*, 12 May 2021; *National Defense Authorization Act for Fiscal Year 2022*, 27 December 2021; *OMB M-22-09*, 26 January 2022; *National Defense Strategy*, 22 March 2022; *National Security Memorandum 8, Task 3: National Manager for National Security Systems Requirement Exception Provision Process (NMM-2022-03)*," 25 February 2022, and others.

The *DoD Zero Trust Strategy* is part of a family of strategies depicted in **Figure 2** below.[21]

Figure 2. Alignment with National and DoD Strategies



The DoD Zero Trust Strategy also provides the foundation for refinements to the *DoD Cybersecurity Reference Architecture (CS RA)*[22] and *DoD Zero Trust Reference Architecture Version 2.0 (ZT RA v2.0)*[23], as well as Component-level strategies and ZT execution plans.

Vision

DoD Zero Trust Strategic Vision

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

The Department envisions a scalable, resilient, auditable, and defendable environment centered on securing and protecting all DoD DAAS in cyberspace.

This strategy establishes the ZT goals and objectives needed within the five-year planning horizon of the Future Years Defense Program (FYDP) starting in FY2023 to FY2027 and beyond. To accelerate the adoption of the full set of ZT capabilities, the Department is also considering several courses of

[21] DoD CIO releases an annual update to the *Capability Planning Guidance (CPG)* which supports each of the strategies identified. There are two additional strategies in draft format as of this publication: *Information Security Continuous Monitoring (ISCM)* and *Endpoint Security (ES)*.
[22] *DoD Cyber Security Reference Architecture*, version 4.2, approval, January 2022.
[23] *DoD ZT RA v2.0*, July 2022.

action (COAs) to include commercial and Government-owned cloud-based enterprise services. These and other adoption acceleration opportunities, including compressed or accelerated execution timelines, will be iteratively defined, developed, and deployed as part of future strategy execution.

The DoD IE and, specifically, the DODIN's cybersecurity capabilities must be able to prevent malicious actors from affecting DoD's ability to detect, deter, deny, defend, and recover from malicious cyber activity across all operational environments.

The Target Level ZT[24] is the minimum set of ZT capability outcomes and activities necessary to secure and protect the Department's DAAS to manage risks from currently known threats. While the DoD ZT Framework will mature and adapt over time, the current strategic context dictates an immediate focus on expediting investments in core ZT capabilities and technologies. The Department and its Components must achieve the Target Level ZT as soon as possible.

With the Target Level ZT achieved, the ZT PfMO will monitor continued compliance and guide movement to Advanced ZT as DoD mitigates current risks. Based on the need to continue the evolution towards a next-generation security architecture and address new threats as malicious actors adjust to DoD's improved security posture, the ZT PfMO may also modify how this strategy defines the Target Level ZT. Using a phased approach to achieve all targeted ZT capabilities will make realizing the Vision of the *DoD Zero Trust Strategy* possible.

[24] Capabilities and activities required to achieve Target Level are depicted in Appendix A-D; includes basic and intermediate Zero Trust maturity as defined by the ZT RA.

Strategic Outcomes

Achieving the *DoD Zero Trust Strategy* results in several significant benefits to the Department, its Components, its partners, and most importantly – the warfighter – in executing missions.

These benefits include:

- The ability of a user to access required data from anywhere, from any authorized and authenticated user and device, fully secured.
- Secured and protected information systems facilitating the Department's evolution into a more agile, more mobile, cloud-supported workforce.
- Reduced attack surface risk profiles through protective actions enabled by micro segmentation of the DoD IE.
- Threats to Cloud, Artificial Intelligence (AI), and Command, Control, Communications, Computers, and Intelligence (C4I) remediated through risk-based cybersecurity protocols and policies.
- Effective damage containment, mitigation, and remediation when a device, network, user, or credential is compromised.
- Consistent, aligned, and effectively resourced ZT capabilities for advanced cybersecurity operations.
- A resilient DoD IE that recovers rapidly from attacks and minimizes damage through enablement of ZT.

Increasing Accessibility:
User Checks and Balances

Challenge: Warfighter interoperability and missions require a wide spectrum of partners, including DIB users, to access DoD networks safely and securely. Authorization to be on and authentication to get onto networks both need to occur. Simultaneously, DoD must institute safeguards to keep malicious actors out – whether state-sponsored seeking intellectual property or persons with malicious intentions.

Pre-ZT Architectures: Attempts to "lock-down" networks (e.g., from certain locations or time periods) and/or to overly restrict access to essential data (e.g., data base or file restrictions) hinder collaboration between DIB users. This increasingly occurs out of an abundance of caution to keep malicious actors out – and impacts interoperability at all mission levels.

Post-ZT Architectures: Adoption of a new, Zero Trust cybersecurity approach results in an effective set of checks and balances. DIB users located overseas and working outside "normal" business hours now can quickly gain authorization to access a sensitive network once they are authorized and authenticated successfully. This enables partners to access data WHEREVER and WHENEVER needed.

DoD Zero Trust Approach

The approach to adopt and accelerate the DoD ZT Framework includes a set of key assumptions and principles that guide execution of the strategy. This Framework outlines an official blueprint to modernize cybersecurity for the DODIN enterprise NIPRNet and SIPRNet. This Framework, based on the seven DoD Zero Trust Pillars, describes how the Department will achieve ZT by providing the foundation and the direction to help align ongoing and future ZT-related efforts, investments, and initiatives across all elements of Doctrine, Organization, Training, materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTmLPF-P). This strategy recognizes that the adoption of ZT will require changes in DOTmLPF-P not only across the Department but also in its Components, to be addressed in their ZT execution plans.

Strategic Assumptions

The following core assumptions drive Department-wide planning for the successful implementation of ZT.[25]

- **Complex Security Threats Persist.** DoD and Components must accelerate ZT implementation and migrate DoD environments to the ZT Framework as quickly as possible to proactively stay ahead of all threat actors and hostile environments, including cyber criminals, nation-state sponsored disrupters, and malicious insiders. As DoD mitigates current weaknesses, new threats will always develop, necessitating course corrections and the ongoing necessity of Zero Trust "station-keeping" to maintain maximum Zero Trust discipline in a strategic and tactical sense.
- **Culture, not just Technology.** 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.
- **Modernization Requires Rethinking.** "Implementing ZT requires rethinking how we utilize existing infrastructure to implement security by design in a simpler and more efficient way,"[26] all while improving warfighter performance, increasing interoperability, and enabling unimpeded operations and resiliency.

Increasing Interoperability:
Secured Network Communications

Complex and fragmented information systems environments plague Warfighters on the ground. The varying controls, inconsistent policies, and manual processes make obtaining access to the applications and data they need to support us in the fight a long and cumbersome process. Zero Trust-based Department architectures, communications and other networks used by our warfighter Coalition partners will enhance connectivity across our Joint Force Command and Control environments, enable rapid integration of communications systems, and facilitate access and sharing of large volumes of secure, actionable data.

[25] See DoD ZT RA, v2.0 for additional design-level assumptions and constraints (Section 1.7 – 1.9, pp. 19-20).
[26] DoD ZT RA, v2.0, July 2022 (Section 2.1, p.20)

- **Increasing Global and Industry Partner Collaboration.** Access to mission information systems and mission partner interoperability are becoming increasingly important as the DIB and foreign partners are significant to coalition warfare and the Joint Warfighting Concept (JWC).[27] Information and data must be effectively shared, accessed and protected based on user attributes, operational need, and delivered by least privilege policies.
- **Concurrent Enterprise and Mission Owner Implementation.** ZT must be implemented concurrently across all levels of the Department, enterprise-wide and orchestrated across DoD and its Components to preclude mission, organizational, governance, and technical silos. ZT must be driven by a unified Enterprise policy that accounts for varied capabilities and associated decisions across the combination of both Enterprise-level and Mission Owner-level interests.
- **Real-time, Risk-based Response.** ZT accelerates the shift from compliance-based to risk-based security approaches as the complexity of threats and vulnerabilities increases. This acceleration is imperative to address future performance and interoperability expectations for initiatives such as JADC2.
  Legacy IT Remains a Challenge. Not every legacy infrastructure and system will require or justify an immediate and/or complete ZT retrofit. However, appropriate security controls must be designed and enforced to counter new cyber attack vectors and emerging threats until a full rationalization of those systems can be conducted to either eliminate or modernize accordingly.[28]
- **Leadership and Operator Buy-in.** Clear direction and adoption across the ZT Ecosystem, from technical, DOTmLPF-P, and functional leaders to operators of the information systems, is vital for a successful enterprise ZT strategy.

Understanding What Devices Need Protected

Challenge: *The expansion in the number of devices, machines, and other NPEs on the DODIN combined with the significant challenge of verifying changes to hardware, firmware, and software increases daily.*

Pre-ZT: The absence of a robust, modern cybersecurity strategy puts systems administrators in an unenviable position of constant worry. They do not fully understand what is on the network nor are they able to ensure those devices do not threaten the security and functionality of transport services.

Post-ZT: Now that ZT is fully implemented across the DODIN, all NPEs are checked and verified at multiple points prior to them being allowed to get onto or remain connected to the system. Systems Administrators now check that everything on the network is appropriately patched and updated, nothing has been unknowingly changed or modified, and everything on the network is fully enrolled. Because this is done on a real-time, automatic basis, systems administrators can now focus on items of highest-risk and have a fighting chance to stay ahead of threats as they mutate and/or persist.

Strategic Principles

A series of guiding principles provide guardrails or parameters for DoD and Component leaders when making decisions regarding how best to implement the strategy and execute the ZT Capability Execution

[27] Joint All Domain Command and Control (JADC2), Mission Partner Environment (MPE) and several other initiatives support the JWC.

[28] For infrastructure or systems unable to comply with mandated ZT adoption, Components and system owners must submit on an annual basis any request for waiver to the ZT PfMO for DoD CIO approval. See "Execution Approach" (page 16 in this document) for additional information. In addition, per the *2022 National Defense Authorization Act* " Not later than 270 days after the date of the enactment of this Act, the Secretaries of the Army, Navy, and Air Force shall each initiate efforts to identify legacy applications, software, and information technology with their respective Departments and eliminate any such application, software, or information technology that is no longer required."

Roadmap. These principles will guide the creation and revision of strategy, policy, design, and execution documents.

- **Mission-Oriented**
  - *Hybrid Work and Location Agnostic*. All users and non-person entities (NPEs) must access, collaborate, work, and execute missions on any network where they both have the need and right to access, governed with least privilege, from any location, based on dynamic credentials, governed by principles of least privilege and safeguarding information.
- **Organizational**
  - *Presume Breach*. Limit the "blast radius" – the extent and reach of potential damage incurred by a breach – by segmenting access, reducing the attack surface, and monitoring risks in real-time within DoD's risk tolerance levels and thresholds. [29]
  - *Incorporate DOTmLPF-P*. 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 DOTmLPF-P. [30]
- **Governance**
  - *Simplify and Automate.* Establish appropriate governance controls that continuously modernize the existing fragmented approaches to data management, IT modernization, and cybersecurity policies and solutions.
  - *Never Trust, Always Verify Explicitly*. Treat every user, device, and application as untrusted and unauthenticated. Authenticate and explicitly authorize to the least privilege using dynamic security policies.
- **Technical**
  - *Least Privilege*. "Subject/entity should be given only those privileges needed for it to complete its task".[31]
  - *Scrutinize and Analyze Behavior*. All events within our IE must be continuously monitored, collected, stored, and analyzed based on risk profiles and generated in near-real time for both user and device behaviors.
  - *Architectural Alignment*. ZT design and architectures must align with the DoD Zero Trust Reference Architecture (ZT RA) design tenets[32] and Committee on National Security

---

[29] "Presume Breach" is defined as "Consciously operate and defend resources with the assumption that an adversary has presence within your environment. Enhanced scrutiny of access and authorization decisions to improve response outcomes". See *DoD ZT RA v2.0*, July 2022, p. 21.

[30] DOTmLPF-P analysis is the first step in Functional Solutions Analysis. It determines/recommends if a non-material approach or a material approach is required to fill a capability gap identified in the Functional Needs Analysis.

[31] The concept of least privileged access" refers to eliminating "the idea of trusted or untrusted networks, devices, personas, or processes, and shifts to multi-attribute-based confidence levels that enable authentication and authorization policies." See *DoD ZT RA v 2.0*, July 2022 v. 2 p. 14.

[32] *DoD ZT RA, v.2.0*, p.21 delineates five (5) tenets that represent the foundational elements and influence all aspects with ZT. These include: 1) Assume a Hostile Environment; 2) Presume Breach; 3) Never Trust, Aways Verify; 4) Scrutinize Explicitly; and 5) Apply Unified Analytics.

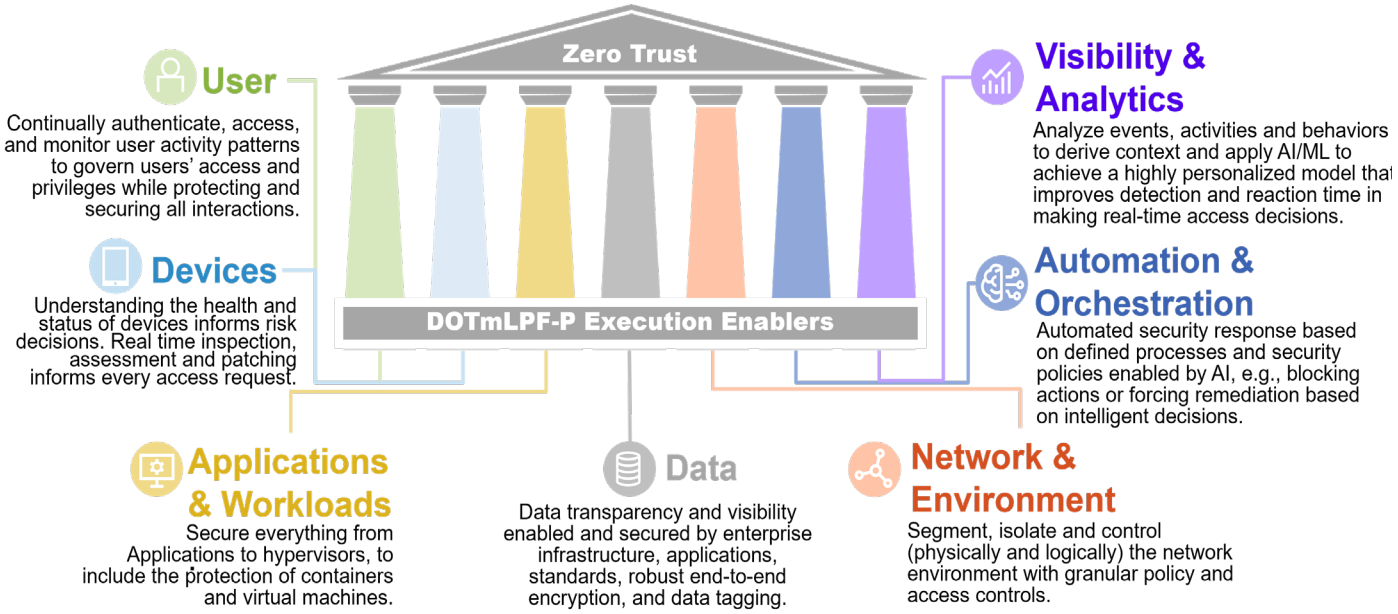
Systems Policy 21 (CNSSP 21), and account for the National Institute of Standards and Technology's (NIST) ZT tenets.[33]

- *Reduce Complexity.* Align technical and security programs with ZT goals and mission objectives to streamline regulations and standards for managing security and risk.

DoD Zero Trust Pillars

Zero Trust capabilities across the IE must be developed, deployed, and operated within an organizing construct defined by seven DoD Zero Trust Pillars and their enablers to ensure standardization of execution. These pillars, as depicted in **Figure 3**, provide the foundational areas for the DoD Zero Trust Security Model and the DoD Zero Trust Architecture.[34] The execution enablers are cross-cutting, non-technical capabilities and activities that address culture, governance, and elements of DOTmLPF-P (e.g., ZT Training, etc.).[35] This ZT security model re-thinks the implementation of security access to resources and is determined by dynamic policy, including observable state of user

Figure 3. DoD Zero Trust Pillars



[33]The seven tenets of zero trust are outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, Zero Trust Architecture, p. 6. These include: 1) All data sources and computing services are considered resources; 2) All communication is secured regardless of network location; 3) Access to individual enterprise resources is granted on a per-session basis; 4) Access to resources is determined by dynamic policy; 5) The enterprise monitors and measures the integrity and security posture of all owned and associated assets; 6) All resource authentication and authorization are dynamic and strictly enforced before access is allowed; 7) The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.

[34] See the DoD ZT RA, v2.0, Sections 2.2 – 2.3, pp. 20 - 23 for a more detailed explanation of the DoD ZT Security Model, the strategic benefit for each pillar and the intended result of all seven pillars working together.

[35] Details regarding supporting enablers will be further refined and integrated into next versions of the *DoD ZT Capability Roadmap* and addressed in implementation plans. Enablers identified to-date include: ZT Awareness & Culture, Adaptive Implementation Governance, ZT Policy Framework, ZT Training, and others.

and endpoint identity, application/service, and the requesting asset. All capabilities within the Pillars must work together in an integrated fashion to secure effectively the Data Pillar, which is central to the model.

Strategic Goals and Objectives

The four high-level strategic goals and their corresponding objectives define what the Department will do to achieve its vision for ZT.[36] These goals are synergistic and address the cultural, technological, and environmental requirements for the successful adoption and implementation of ZT. They align with and informed by the strategic assumptions, priorities, and principles. Each goal in **Table 1** has accompanying SMART (specific, measurable, achievable, relevant, and time-bound) objectives that direct what specific actions Mission Owners at all levels must do.[37]

Table 1. Key Benefits of Realizing ZT Strategic Goals & Objectives

Goal	Impact to Warfighters / DoD / Components & Partners
1: Zero Trust Cultural Adoption	• A cybersecurity-minded culture and workforce that embraces ZT • Increased collaboration and productivity • Increased commitment to cybersecurity
2: DoD Information Systems Secured and Defended	• Secured communications at all operational levels • Improved systems performance • Interoperable & secured data • Automated cyber and AI operations
3: Technology Acceleration	• Continually updated & advanced ZT enabled IT • Reduced silos • Simplified architecture • Efficient data management
4: Zero Trust Enablement	• Enhanced operations and support performance • Consistent, aligned, and effectively resourced ZT supporting functions • Speed of ZT acquisition-to-deployed capability

[36] The strategic goals and corresponding objectives as listed are not prioritized. Rather, each needs to be accomplished to meet the ZT *Vision*.
[37] While the objectives prescribe "what" shall be done in furtherance of the goal, they do not prescribe "how," as DoD Components may need to undertake objectives in differing ways.

Goal 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.*

All DoD personnel are aware, understand, commit to, and trained to embrace a ZT mindset and culture[38] and support integration of ZT technologies in their environments that includes cross-cutting DOTmLPF-P enablers

Goal 2: DoD Information Systems Secured and Defended. *DoD cybersecurity practices incorporate and operationalize Zero Trust to achieve enterprise resilience in DoD information systems.*

Components apply the DoD ZT Framework to all new and legacy information systems and achieve the capability outcomes prescribed by the *DoD Zero Trust Capability Roadmap*[39] and aligned to the cyber resiliency focus of the *National Defense Strategy 2022*. Component level execution plans provided to DoD CIO and Joint Force Headquarters – Defense Information Networks (JFHQ-DODIN) through the DoD ZT PfMO no later than 23 September 2023 will address how Zero Trust is applied across their networks, including all infrastructure and systems.[40] Additionally, Components must achieve the intended Target level outcomes of each DoD Zero Trust Capability and execution enabler no later than the end of FY2027. Together, these outcomes support the strengthening of the joint development, operational testing, and existing interoperable capabilities that enhance DoD, Mission partner, and warfighter ability to operate and achieve secure command and control communications from the national level to the warfighter.[41]

Goal 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.*

The DoD IE and DODIN are secured and defended quickly and effectively (i.e., Goal 2), and include the best and most up to date technologies that allow for scaling, amplifying, and failing fast for innovation. The Department and Component architectures align with ZT efforts, include

---

[38] Outcomes of Goal 1 also align with two (2) of the five (5) lines of effort defined in the 2018 *DoD Cyber Strategy*: "Reform the Department" and "Cultivate Talent." See *Summary: DoD Cyber Strategy*, 2018, pp. 5-6.
[39] The *DoD Zero Trust Capability Roadmap* was developed in conjunction with this Strategy.
[40] The *2022 National Defense Authorization Act*, Section 1528 (d) requires "not later than one year after the finalization of the zero trust strategy, principles, and model architecture . . . the head of each component of the Department of Defense shall transmit to the Chief Information Officer of the Department and the Commander of the 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." [41] Outcomes of Goal 2 also align with two (2) of the five (5) lines of effort defined in the 2018 *DoD Cyber Strategy*: "Build a More Lethal Joint Force" and "Compete and Deter in Cyberspace." See *Summary: DoD Cyber Strategy*, 2018, p. 4.
[41] Outcomes of Goal 2 also align with two (2) of the five (5) lines of effort defined in the 2018 *DoD Cyber Strategy*: "Build a More Lethal Joint Force" and "Compete and Deter in Cyberspace." See *Summary: DoD Cyber Strategy*, 2018, p. 4.

development testing, and ensure interoperable standards and assets. These efforts apply across the DoD IE.[42]

Goal 4: Zero Trust Enablement. *DoD Zero Trust execution integrates with Department-level and Component-level processes resulting in seamless and coordinated ZT execution.*

Processes, policies, and funding are necessary to ensure that the ZT Framework is cemented across the DoD IE. This means Department-level and Component-level processes and resources must be reimagined or synchronized with ZT principles and approaches. This resourcing is sustainable and built-in to adjacent, complementary, and synergistic DoD technology, information security, and budgeting efforts and initiatives. This goal identifies the "tail" to the ZT "tooth," the latter being unable to achieve its mission without the former, and requires the whole of the ZT Ecosystem's attention and effort and cannot be addressed "at a later time."[43]

See **Figure 4** below for descriptions of the objectives needed to achieve each goal.

[42] Outcomes of Goal 3 also align with two (2) of the five (5) lines of effort defined in the 2018 *DoD Cyber Strategy*: "Build a More Lethal Joint Force" and "Strengthen Alliances and Attract New Partnerships." See *Summary: DoD Cyber Strategy*, 2018, pp. 4-5.

[43] Outcomes of Goal 4 also align with one (1) of the five (5) lines of effort defined in the 2018 *DoD Cyber Strategy*: "Reform the Department." See *Summary: DoD Cyber Strategy*, 2018, pp. 5-6.

Figure 4. DoD Zero Trust Strategy Goals and Objectives

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*
Objectives	**1.1 Commitment.** Transform DoD cybersecurity to a ZT framework that is universally understood, accepted, and embraced by DoD Components Start: FY2023	**2.1 User.** Secure, limit, and enforce strong authentication of person and non-person entity access	**3.1 Capabilities.** Achieve intended outcomes for ZT capabilities aligned with planned increments as described in the DoD ZT Capability Implementation Roadmap through end of FY2027	**4.1 Policy.** Establish a unified policy and other guidance to integrate the latest tested and proven cybersecurity best practices, standardize management of requirements, and share best practices by end of FY2023 and refine iteratively through FY2027
	1.2 Outreach. Conduct a comprehensive ZT outreach initiative to inform and share data from ZT efforts and to define standards, minimize duplications, emphasize successes, and to facilitate an open exchange of information sharing with DoD, federal, and academia partners by end of FY2023, and iteratively updated through FY2027	**2.2 Device.** Identify, inventory, authorize, authenticate, and patch all devices continuously and in real-time	**3.2 Architecture:** Align, update, and maintain agile-based reference architectures and research, development, and engineering efforts with ZT architecture principles by end of FY2023	**4.2 Planning.** Incorporate ZT requirements into DoD-wide and Component-specific strategies, policies, frameworks, and directives, and contracts by end of FY2023 and next iteration through FY 2027
	1.3 Awareness. Implement internal and external communication campaigns at all levels, including with the DIB and foreign allies as appropriate, to include Department-wide advocacy, awareness, and support for the implementation of the DoD ZT strategy goals and objectives by end of FY2023, and iteratively updated through FY2027	**2.3 Applications & Workloads.** Secure all applications and workloads, to include the protection of containers and virtual machines	**3.3 Interoperability.** Ensure the compatibility and integration of established institutionalized standards, leverage assets and knowledge, and ensure compatibility between DoD information systems and across the DoD IE by end of FY2024	**4.3 Programming.** Align DoD Future Years Defense Program (FYDP) to adequately support execution of the ZT Implementation Roadmap by FY2023 and updated iteratively through FY2027
	1.4 Workforce. Identify and develop a cadre of ZT professionals by end of FY2025	**2.4 Data.** Enable and secure data transparency and visibility with enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging	**3.4 Ideation / Innovation.** Vet, scale and amplify emerging practices, concepts, and technologies through pilots and fast-fail, employing best practices and lessons learned, on-going through FY2027	**4.4 Funding.** Resource through the FYDP process the ZT capabilities, technologies, and initiatives by end of FY2027
	1.5 Training. Embed ZT training across DoD Components, related workforce requirements, and certification standards by end of FY2024	**2.5 Network & Environment.** Segment (both logically and physically), isolate, and control the network/environment (on-premises and off-premises) with granular access and policy restrictions		**4.5 Acquisition.** Develop a plan to acquire and deploy solutions and technologies that advance ZT by early FY2023 and refine iteratively through FY2027
		2.6 Automation & Orchestration. Automate manual security and other applicable processes to take policy-based actions across the enterprise with speed and at scale		**4.6 Performance.** Measure ZT capability deployment and maturity through key performance indicators and associated metrics to monitor and advance ZT execution through FY2027
		2.7 Visibility & Analytics. Analyze events, activities, and behaviors to derive context and apply AI/ML to achieve models that improve detection and reaction time in making real-time access decisions		**4.7 Zero Trust PfMO.** Mature the ZT PfMO by end of FY2023 to act as a trusted partner for orchestrating ZT across the DoD IE and to provide strategic oversight, execution direction, and resource priorities to accelerate ZT adoption

**Note: See the ZT Capability Roadmap for timeline to achieve objectives in this Goal*

Execution Approach

The Department will achieve the ZT goals and objectives at the accelerated pace envisioned through continual, adaptive, and centralized coordination of strategic guidance, resource prioritization, and alignment of enterprise-wide and Component-specific efforts. Achieving these goals and objectives requires a multi-pronged approach that goes beyond technology solutions to address people, processes, resources, governance, and risk management, among others. Specifically, the Department and its Components will plan for and address all elements of ZT DOTmLPF-P solution gaps. Resources will be aligned to diminish identified gaps and result in the ZT Framework across the Department that meets national strategic guidance, protects national interest, and reduces malicious actors. The path to achieving impactful security benefits with ZT is through an iterative process that must be continuously refined as the strategic context evolves as DoD and its Components execute their action plans, and federal guidance evolves. The Department will periodically reevaluate the effectiveness of its strategy and make course adjustments as needed.

Acting on behalf of the DoD Cyber Council and through applicable DoD offices of primary responsibility and in coordination with the Components, the Director of the ZT PfMO orchestrates overall strategy execution. The PfMO will work closely with Components to define, develop, and adapt execution plans to achieve each of the goals and objectives outlined in **Figure 4**.

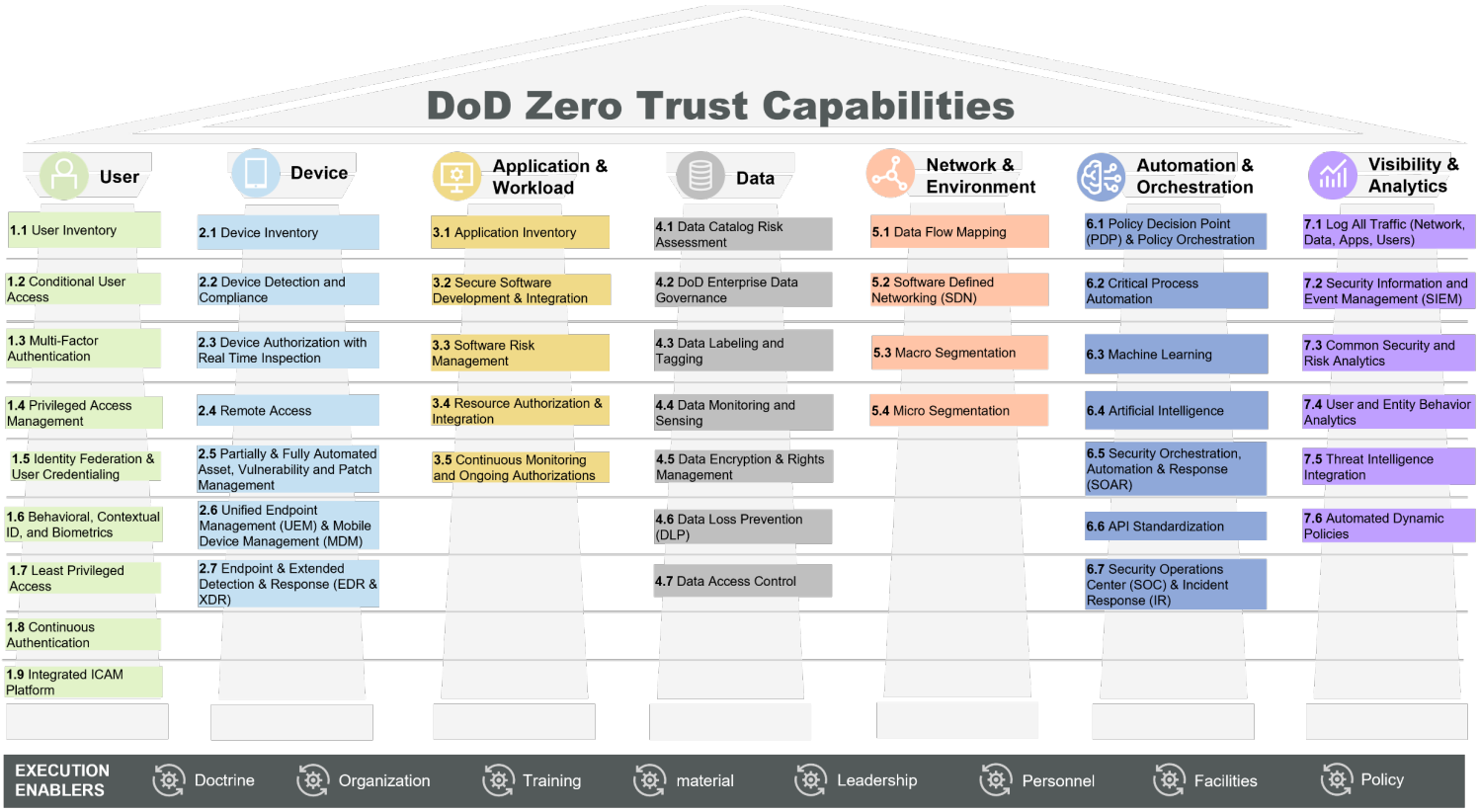
The starting point for ZT and maturity levels vary across the DoD IE due to completed, ongoing, and planned initiatives. Moving forward, Components must align their execution plans to this strategy to achieve the outcomes and identify implementation opportunities and obstacles.

Legacy infrastructure and systems may not require or justify immediate ZT retrofit and depending on where and how installed, may not comply with mandated ZT adoption. Components and system owners must submit on an annual basis any request for waiver to the ZT PfMO for DoD CIO approval based on a pre-defined set of standards designed to ensure maximum security of DoD networks.

System owners are responsible for executing and enforcing the move to ZT and must understand risks associated with delaying implementation. Appropriate security controls, including potential refinements to how DoD implements the Risk Management Framework (RMF), must be designed and enforced to counter new attack vectors and emerging threats until a full rationalization of those systems can be conducted to either eliminate or modernize accordingly.

In addition, Components must determine their intent to adopt enterprise solutions that comply with the ZT RA and DoD CIO guidance. To achieve a fully secured and defended DoD IE (Goal 2) the Department and Components must achieve all ZT capabilities shown in **Figure 5**.

Figure 5. DoD Zero Trust Capabilities



The Department and its Components must achieve the DoD "Target Level ZT" as soon as possible. Target Level ZT includes the minimum set of ZT capability outcomes and activities necessary to secure and protect the Department's DAAS to manage risks from currently known threats. It is the level set by the DoD ZT PfMO to which all of DoD must minimally achieve.

With the Target Level achieved, the ZT PfMO will monitor continued compliance and guide movement to Advanced ZT as current risks are mitigated. Advanced capabilities include the complete set of identified ZT capability outcomes and activities that enable adaptive responses to cybersecurity risk and threats and offer the highest level of protection. Although a limited number of systems and DAAS will be specifically required to achieve this advanced level within the timeframe of this strategy, DoD will continue to seek the adoption of the advanced capabilities as outlined in Appendix B and C. Reaching an "advanced" state (Advanced ZT) does not mean an end to maturing ZT; instead, protection of attack surfaces will continue to adapt and refine as the malicious actors methods advance and mature.

Based on the need to continue the evolution towards a next-generation security architecture and address new threats as malicious actors adjust to the DoD's improved security posture, the ZT PfMO may also modify how this strategy defines the Target Level ZT.

Resourcing and acquisition guidance will ensure ZT capabilities and activities are sufficiently contracted, received and deployed within schedules required for the DoD to meet ZT deployment timelines across the DODIN enterprise. Strategy measures will provide a means to assess ZT

execution and effects. The governance concept will delineate roles and decision rights for implementation.

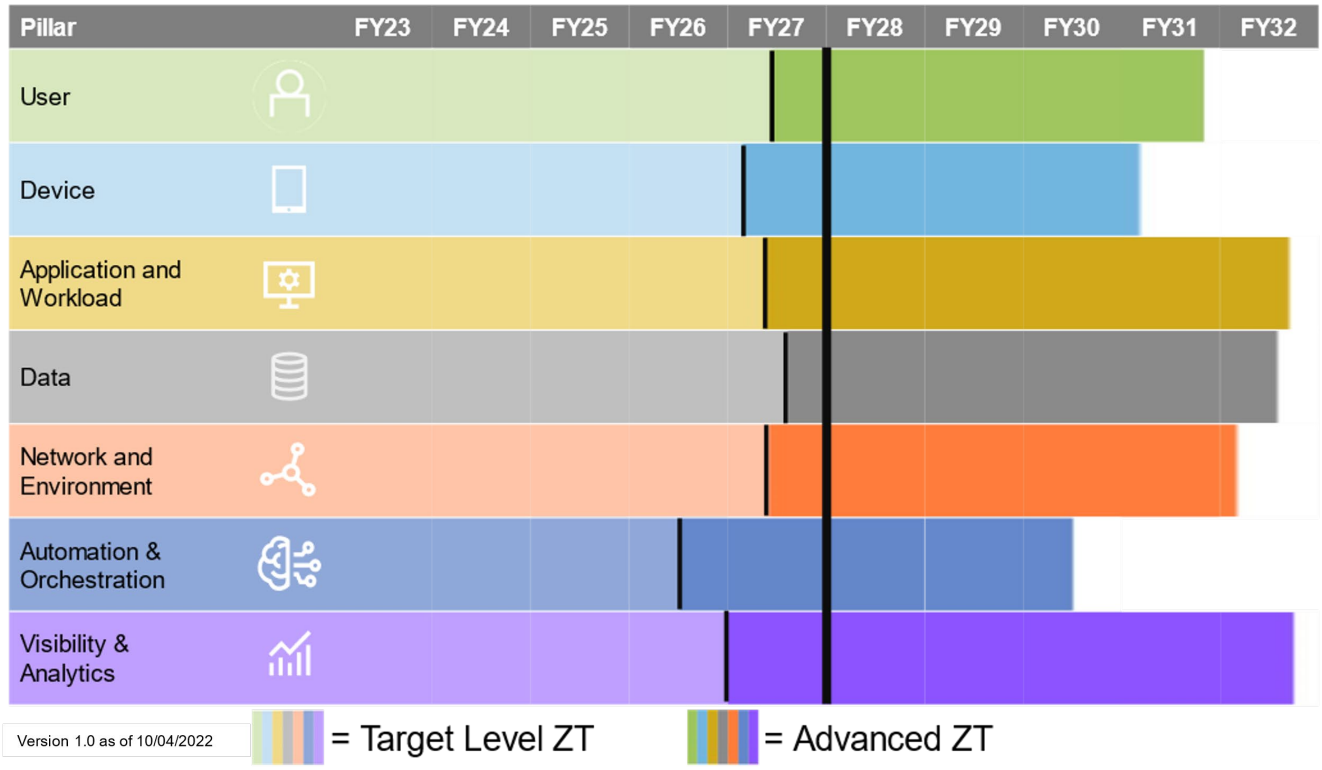
The *DoD Zero Trust Capability Roadmap* described in the High-Level Capability Roadmap section below provides a guide to follow for the DoD baseline course of action (COA).[44] Additionally, to accelerate Zero Trust adoption, the Department is considering several additional complementary COAs including commercial and Government-owned cloud-based enterprise services. These and other adoption acceleration opportunities, including compressed or accelerated execution timelines, will be iteratively defined, developed, evaluated, and deployed as part of future strategy execution.

High-Level Capability Roadmap

The *DoD Zero Trust Capability Roadmap* describes how the Department currently envisions achieving the capability-based outcomes and activities sequenced over time to achieve the DoD Target Level ZT and Advanced ZT.[45] The *Roadmap* outlines dependencies and interdependencies affecting sequence and parallel development and provides a general timeline to achieve outcomes by fiscal year. **Figure 6** provides a high-level depiction of a brownfield approach and shows when outcomes for each capability by pillar should be achieved, beginning in FY23 with Target Level ZT achieved by FY27.[46] See **Appendices A - D** for details on when each ZT capability and supporting activity should be achieved. Components will determine how (e.g., technologies, solutions, etc.) these outcomes will be achieved and develop associated action plans.

[44] The *DoD Zero Trust Capability Execution Roadmap, v1,* developed by the ZT PfMO will be finalized in parallel with this *Strategy* in Summer, 2022. The *Roadmap* includes descriptions of each capability outcome.
[45] Although the full set of DoD ZT Capabilities span from target to advanced, some capabilities are achieved at the target level, and a few are strictly advanced. The majority of capabilities have associated activities that include both ZT Target Level and Advanced ZT.
[46] Determination of Target Level and fiscal year projection is based on the DoD Baseline "COA 1" described in the DoD *Zero Trust Capability Execution Roadmap, v1*.

Figure 6. DoD Zero Trust Capability by Pillar by Fiscal Year



Resourcing & Acquisition

The ZT PfMO serves as the customer-focused, multi-functional team responsible for orchestrating and prioritizing ZT-related resources and acquisition decisions for the Department. In alignment, and in collaboration with other relevant DoD stakeholders, the ZT PfMO will develop strategic guidance and ensure resources are properly managed.

Resourcing

ZT resourcing will be addressed for each organization impacted through a multi-pronged approach; the DoD CIO's Capability Programming Guidance (CPG) and the Planning, Programming, Budgeting and Execution (PPBE) process. This will enable each organization to appropriately identify and prioritize new and existing resources necessary to execute the ZT capability and pillar outcomes defined above (see High-Level Capability Roadmap). At the Enterprise-level, DoD CIO, through the ZT PfMO, will guide ZT resource priorities through the annual CPG to ensure that all efforts across the DoD IE are appropriately aligned with the *Strategy* and *Roadmap*. DoD CIO will work with Components to address any Component-level resourcing shortfalls, each fiscal year, within the annual Program Objective Memorandum (POM) cycle, starting with the next immediate submission. Additionally, DoD CIO will work with Components to submit requests for new funding to Congressional appropriators through the regular DoD resourcing processes.

Acquisition

Developing a ZT acquisition strategy should align with the Department's priority to build a resilient Joint Force and defense ecosystem that involves undertaking reforms to accelerate force development and technology acquisition.[47] DoD CIO will coordinate the identification and determination of the applications, assets, and services that DoD, or designated executive agents, will procure and acquire at the Enterprise-level. Components will be responsible for the overall management and oversight of technology development, acquisition, and product support suitable for their respective missions while ensuring their strategies align with applicable Enterprise-level strategies.

Market research provides necessary information such as: whether products/services required for an acquisition are available in the marketplace, how the marketplace is currently implementing the capabilities, and whether any existing contract vehicles are available to execute and expedite the requirement(s). Additionally, the DIB, as well as research and development labs, Red Teaming, and Operational Test & Evaluation (OT&E) activities, plays a critical role in identifying and demonstrating potential ZT capabilities and solutions that should also be considered.

Depending on their ZT Execution plans, each Component will be responsible for conducting additional market research and requirements definition to determine whether they need to revise their current and/or create new acquisition strategies. Acquisition strategies will ultimately identify existing and/or the need to create new, contract mechanisms to make this a reality.

This ZT strategy does not mandate or prescribe specific technologies or potential solutions. Rather, it describes all the ZT capabilities that must be implemented to reach both the Target and Advanced Level ZT. The Components are free to select their own solutions and solution architectures, as long as they deliver the specified ZT Capability outcomes needed to reach the Target or Advanced Level ZT and are able to show that proof to their Authorizing Official and/or the ZT PfMO. Components must procure and deploy products and solutions that hit target levels. DoD shall define the logical architecture schema against which the macro level cybersecurity polies are consistently aligned and implemented against all environments.

[47] *Fact Sheet: National Defense Strategy*, 28 March 2022.

Measurement and Metrics

To assist in remaining vigilant and accountable to this strategy, the ZT PfMO will develop and deploy a metrics-based approach for measuring and reporting the Department's progress toward meeting the four strategic goals outlined in this strategy. Each goal contains SMART objectives that can be used to measure goal progress. Additional metrics will be required for specific objectives and goals, for example, measurement of the capability implementation according to the Zero Trust Capability Implementation Roadmap. In addition to measuring *DoD Zero Trust Strategy* goals and objectives, metrics will be developed to measure the impact and benefit of what each strategy goal sets out to achieve.

Cybersecurity Operations Visibility

Cybersecurity and intelligence analysts working on the front lines of the Department's security operations centers struggle to maintain an enterprise view of common threats and vulnerabilities and to communicate effectively when incidents emerge. Siloed domains and manual interventions are par for the course in today's conventional architectures and result in increased security risks and inconsistent policies, data, logs, and analytics. With Zero Trust executed, these analysts in the Department's cybersecurity operations centers will have the ability to maintain dynamic security monitoring, receive real-time alerts, and automatic incident response –providing the best chance of keeping malicious actors out, and getting them off DoD's networks.

Employing specific, qualitative, and quantitative metrics to measure Department progress toward achieving the strategic goals is necessary to measure the progress of ZT adoption across DoD, ensure compliance with governance and other standards, align funding and programming, and to provide senior leadership with periodic assessments of the security of the DoD IE.

Measurements and metrics are also critically important to determine the status and effectiveness of ZT implementation and must be available to ascertain what impact and requirements are required. They will be used to validate the security of our systems and networks and specific component level DAAS. Future decisions on the incorporation of ZT technologies and concepts will be informed by ZT measurement.

Each Component shall contribute data to support the analysis of the effectiveness and progress of this strategy. Component reporting requirements will be part of the ZT adoption measurements and metrics. The ZT PfMO will provide the DoD Cyber Council with a combined scorecard to measure this strategic plan's progress and identify additional risks that need to be mitigated to advance overall ZT strategic objectives.

Governance

ZT is governed by existing DoD CIO committee structures as overseen by DoD CIO and JFHQ-DODIN. The DoD Cyber Council (CC) is the primary authority for ZT technical and strategic direction and is co-chaired by the DoD CIO and Principal Cyber Advisor on behalf of the Deputy

Secretary of Defense.[48] The Director of the ZT PfMO acts on CC direction and orchestrates overall ZT strategy execution. This includes providing strategic guidance, directing the alignment of efforts, and prioritizing resources to accelerate ZT adoption across the DoD.[49] The ZT PfMO Director will bring other non-technical decisions to the applicable DoD governance forum or DoD CIO committee.

In support of Department-wide ZT governance, the ZT PfMO develops, issues, and tracks ZT-related governance decisions (including roles and responsibilities), policy, and processes for the Department. It serves as the coordinator for ZT efforts and supports the DoD Cyber Council regarding all matters related to ZT implementation. ZT PfMO guidance will align with all applicable DoD CIO governance and directives.

Summary

Executing and achieving the objectives laid out in this strategy requires the coordinated efforts of the Joint Force and the entire defense ecosystem. Everyone in the Department has a role to ensure the success of ZT. While protecting data is central to ZT, successfully implementing our ZT Framework requires that the entire Department understands and embraces a culture of ZT.

To achieve the DoD Zero Trust Strategic Vision, the Department must pursue the strategic goals outlined above as an enterprise. While this is an enormous task, DoD has already made significant progress. Dating over a decade, DoD has advanced cybersecurity through initiatives such as continuous monitoring, multifactor authentication, and others. The technologies and solutions that create ZT, and the benefits it provides, must become a part of the Department's lexicon and be accounted for in every plan and operation.

Cybersecurity in the world today is, by definition, a moving target, and while it may move, the concept and the culture will remain the same, even as the Department adapts and refines the strategy. Ongoing and open communication and coordination, underpinned by proper funding and resourcing, are key to the strategy's success.

The Department's ability to protect, and by extension, DoD personnel against the array of increasingly sophisticated cybersecurity threats depends on it.

---

[48] The DoD Cyber Council is a "Supporting Tier Forum" as part of the DoD Supporting Tier Governance Forum Structure defined by DOD Directive 5105.79 *DoD Senior Governance Framework*, 8 November 2021, p. 10.
[49] The DoD ZT PfMO capabilities and services are derived from existing DoD CIO authorities. 40 U.S. Code § 11315 assigns general responsibilities, duties, and qualifications to the CIOs of executive agencies. 10 U.S. Code § 142 assigns authorities specifically to the DoD CIO. DoDD 5144.02 (DoD Chief Information Officer) (dtd 11/21/2014; incorporating Change 1 dtd 9/19/2017) assigns the responsibilities, functions, relationships, and authorities of the DoD CIO, pursuant to Title 10 and Tile 40 of the United States Code.

APPENDIX A: DoD Zero Trust Capabilities (Target & Advanced Levels)

Summary. Each DoD ZT Capability aligns to one of the seven DoD ZT Pillars (depicted horizontally). Although the full set of DoD ZT Capabilities span from target to advanced, some capabilities are achieved at the target level, and a few are strictly advanced. The majority of capabilities have associated activities that include both ZT Target Level and Advanced ZT (depicted vertically by the center column). The execution enablers are cross-cutting, non-technical capabilities and activities that address culture, governance, and elements of DOTmLPF-P. Contact the DoD ZT PfMO at osd.pentagon.dod-cio.mbx.zero-trust-portfolio-management-office@mail.mil for outcome descriptions of each capability.

DoD Zero Trust Capabilities (Target & Advanced Levels)

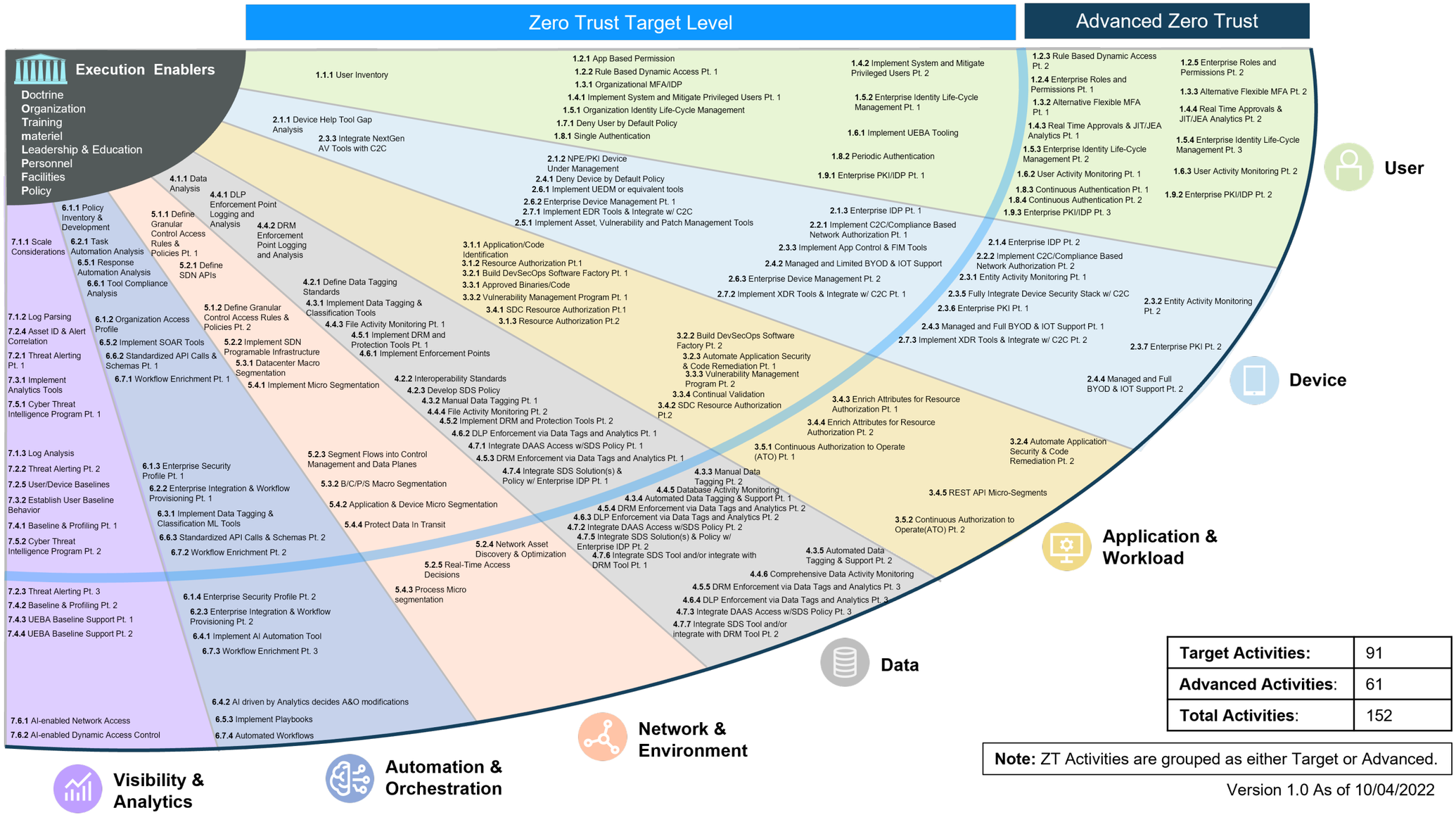
	Target		Target & Advanced		Advanced
User	**1.1** User Inventory	**1.7** Least Privileged Access	**1.2** Conditional User Access **1.3** Multifactor Authentication **1.4** Privileged Access Mgmt. **1.5** Identity Federation and User Credentialing	**1.6** Behavioral, Contextual ID, & Biometrics **1.8** 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** Secure 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	**4.3** Data Labeling & Tagging **4.4** Data Monitoring & Sensing **4.5** Data Encryption & Rights Management	**4.6** Data Loss Prevention (DLP) **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	**6.1** Policy Decision Point (PDP) & Policy Orchestration **6.2** Critical Process Automation	**6.5** Security Orchestration, Automation & Response (SOAR) **6.7** Security Operation Center (SOC) & Incident Response (IR)	**6.4** Artificial Intelligence
Visibility & Analytics	**7.1** Log All Traffic	**7.3** Common Security & Risk Analytics **7.5** Threat Intelligence Integration	**7.2** Security Information and Event Mgmt. (SIEM)	**7.4** User & Entity Behavior Analytics (UEBA)	**7.6** Automated Dynamic Policies

EXECUTION ENABLERS	Doctrine	Organization	Training	materiel	Leadership & Education	Personnel	Facilities	Policy

Version 1.0 As of 10/04/2022

APPENDIX B: DoD Zero Trust Activities (Target & Advanced Levels)

Summary. Each DoD ZT Capability breaks down into a series of associated activities achieved at ZT Target Level (represented by the inner light blue arc) or at Advanced ZT (represented by outer dark blue arc). The execution enablers are cross-cutting, non-technical capabilities and activities that address culture, governance, and elements of DOTmLPF-P. When viewing the illustration electronically, magnify the zoom level to see the title of each activity. When printing, configure the page setting to Ledger (11" x 17"). Security Control overlay is under development; contact the DoD ZT PfMO at osd.pentagon.dod-cio.mbx.zero-trust-portfolio-management-office@mail.mil for outcome descriptions of each activity.



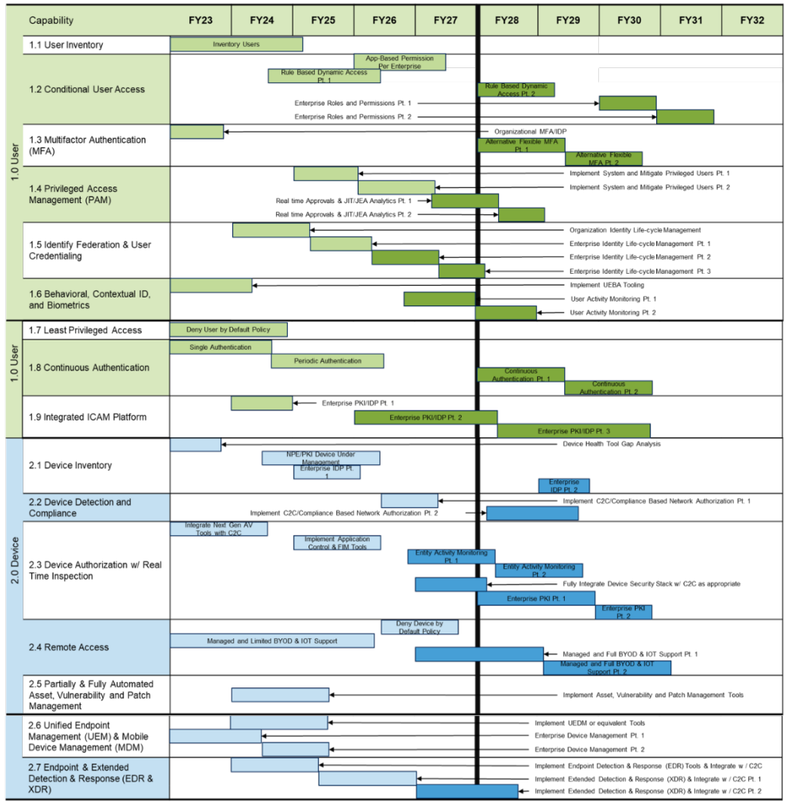
Target Activities:	91
Advanced Activities:	61
Total Activities:	152

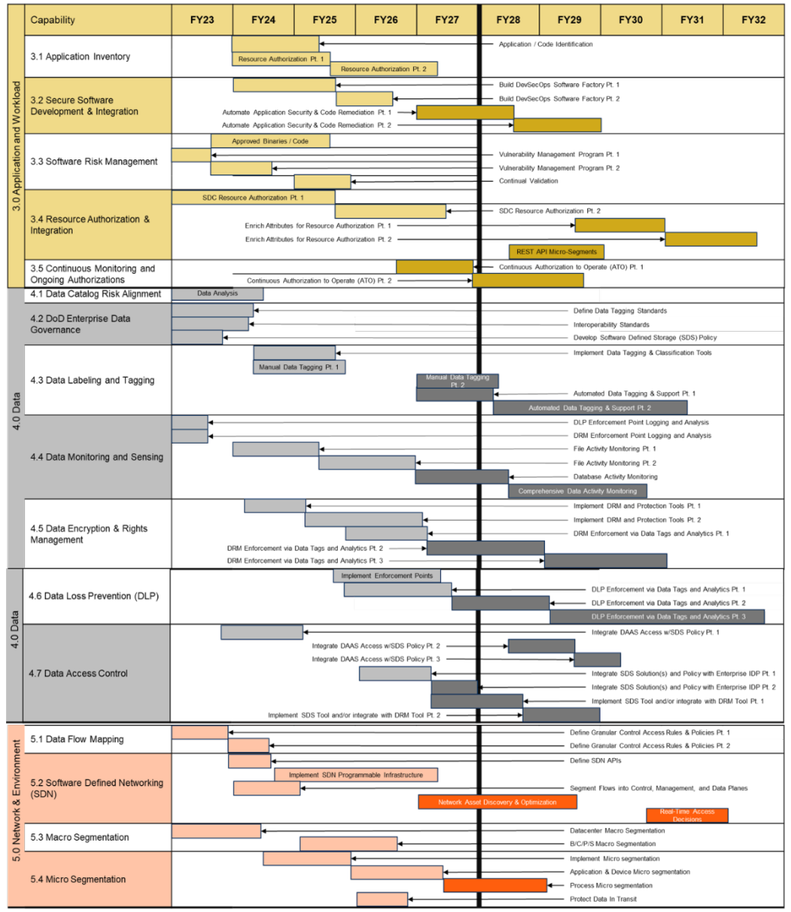
Note: ZT Activities are grouped as either Target or Advanced.

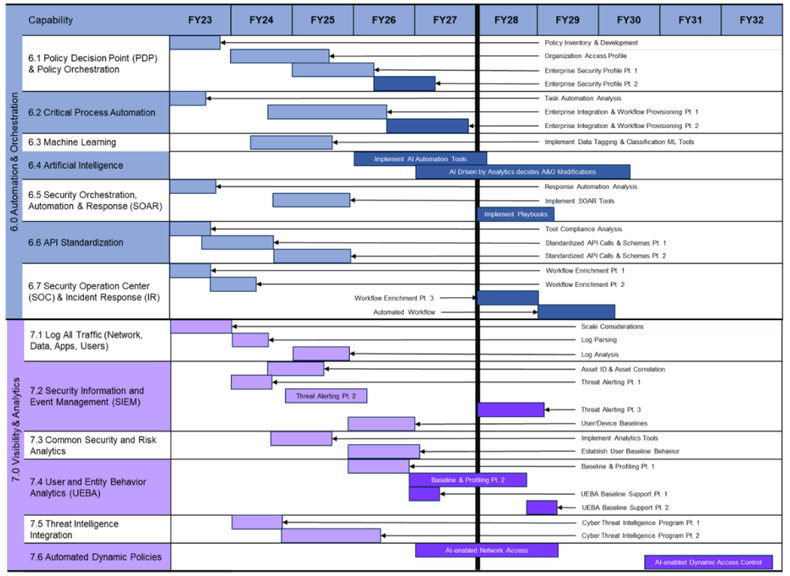
Version 1.0 As of 10/04/2022

APPENDIX C: DoD Zero Trust Capability Roadmap (by Fiscal Year)

Summary. The ZT Capability baseline timelines, depicted by DoD ZT Pillar and Fiscal Year, provide the projected roadmap for achieving the ZT Target Level by the end of FY2027. Each ZT Capability includes its associated predecessor/successor relationships. Capabilities with no predecessors can begin earlier when resourced appropriately. When viewing the illustration electronically, magnify the zoom level to see the title of each capability. When printing, configure the page setting to Ledger (11” x 17”). Contact the DoD ZT PfMO at osd.pentagon.dod-cio.mbx.zero-trust-portfolio-management-office@mail.mil for further information.





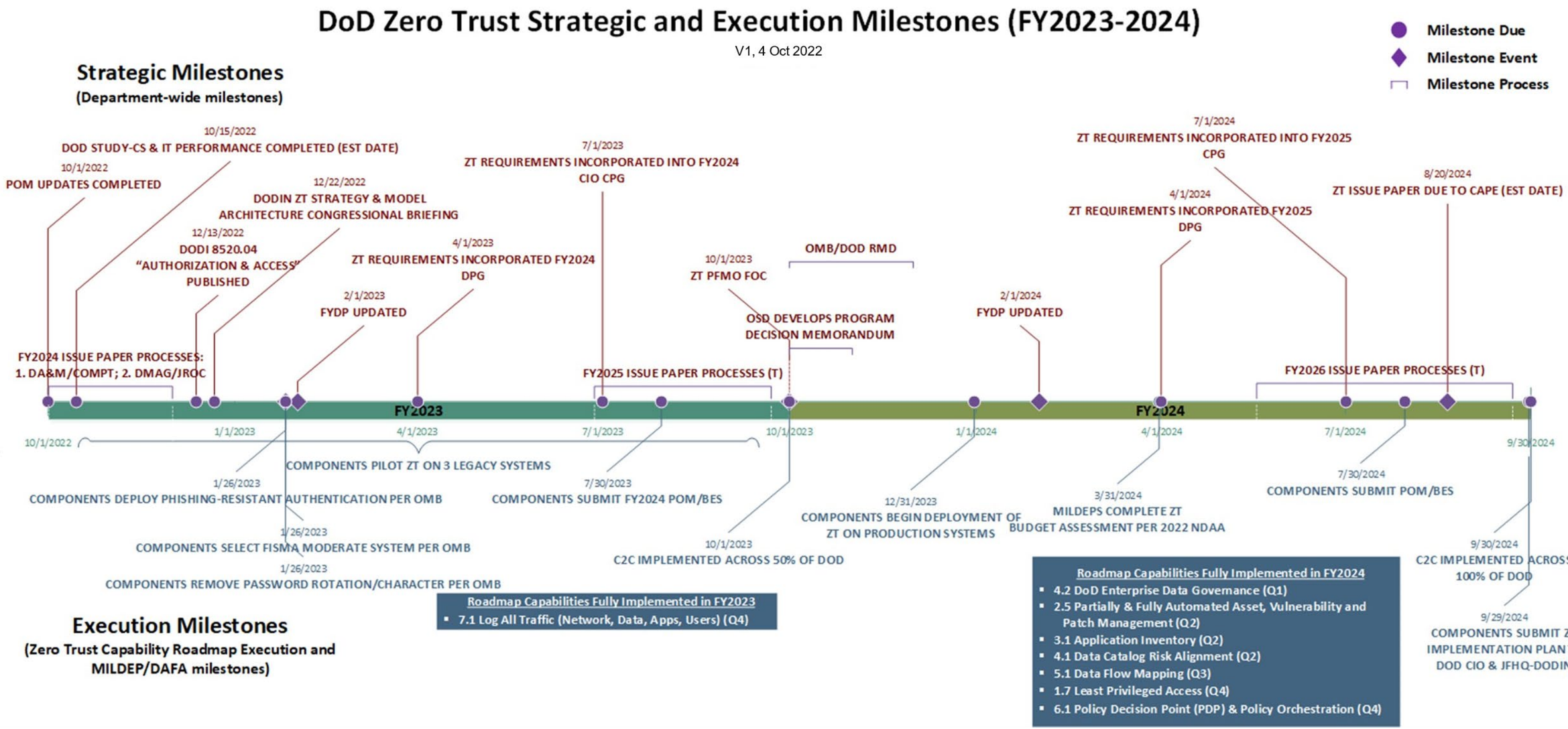


= Target Level ZT

= Advanced ZT

APPENDIX D: DoD Zero Trust Strategic and Execution Milestones (FY2023 – FY2024)

Summary. The *DoD ZT Strategy* implementation timeline below depicts the strategic and execution milestone due dates, events, and processes for FY2023 and FY2024 as currently envisioned. When viewing the illustration electronically, magnify the zoom level to see the title of each milestone. When printing, configure the page setting to Ledger (11" x 17"). Contact the DoD ZT PfMO at osd.pentagon.dod-cio.mbx.zero-trust-portfolio-management-office@mail.mil for further information.



APPENDIX E: References

Table 2. References

Name
Committee on National Security Systems Policy 21, National Cybersecurity Policy on Enterprise Architecture Frameworks for National Security Systems, 30 July 2016
DoD Artificial Intelligence Strategy, 12 February 2019
DoD C3 Modernization Strategy, September 2020
DoD Cloud Strategy, 18 December 2018
DoD Cyber Risk Strategy*
DoD Cyber Security Reference Architecture, version 4.2, January 2022*
DoD Cyber Strategy, September 2018*
DoD Data Strategy, 30 September 2020*
DoD Defense Planning Guidance*
DoD Digital Modernization Strategy, 12 July 2019
DoD Directive 5105.79, DoD Senior Governance Framework, 8 November 2021
DoD Directive 5144.02, DoD Chief Information Officer (DoD CIO), Chg 1, 19 September 2017
DoD Directive 8000.01, Chg 1; Management of the Department of Defense Information Enterprise (DoD IE), Section 2(a), 17 July 2017
DoD ICAM Strategy, 30 March 2020
DoD Instruction (DODI) 5000.82, Acquisition of Information Technology (IT), 21 Apr 2020
DoD OCONUS Cloud Strategy, 26 May 2021
DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs, January 2017
DoD Software Modernization Strategy, 2 February 2022
DoD Zero Trust Reference Architecture, February 2021
Executive Order on Improving the Nation's Cybersecurity, 12 May 2021
Fact Sheet: National Defense Strategy, 28 March 2022
Joint Publication 6-0, Joint Communications System, 10 June 2015 Incorporating Change 1 04 October 2019
National Defense Authorization Act for Fiscal Year 2022, 21 December 2021
National Defense Business Operations Plan, 9 April 2018
"National Security Memorandum 8, Task 3: National Manager for National Security Systems Requirement Exception Provision Process (NMM-2022-03)," 25 February 2022*
"National Security Memorandum 8, Task 4: National Manager for National Security Systems Binding Operational Directive and Emergency Directive Procedures (NMM-2022-04)," 25 February 2022*

**Contact the Zero Trust PfMO at osd.pentagon.dod-cio.mbx.zero-trust-portfolio-management-office@mail.mil if you require access to classified, FOUO, or CUI documents marked with an asterisk*

Table 2. References (cont.)

Name
"(U//FOUO) National Security Memorandum 8, Task 5: Identification and Inventorying of National Security Systems Guidance (NMM-2022-05)," 25 February 2022*
"National Security Memorandum 8, Task 6: Multifactor Authentication and Encryption for National Security Systems Data Guidance (NMM-2022-06)," 25 February 2022*
"National Security Memorandum 8, Task 14: National Manager for National Security Systems Request for Technical and/or Operational Assistance Procedures (NMM-2022-14)," 21 April 2022*
National Security Memorandum-8, "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems," 19 January 2022
National Security Strategy, 12 October 2022
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, Zero Trust Architecture, August 2020
National Institute of Standards and Technology (NIST) Special Publication (SP) 1271, Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide (6 August 2021)
"Mission Partner Environment Cuts Decision Making, Kill Chain," DoD News, 29 November 2021
Office of Management and Budget Memorandum M-22-01, "Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response," 8 October 2021
Office of Management and Budget Memorandum M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," 26 January 2022
Summary: DoD Cyber Strategy 2018, September 2018

**Contact the Zero Trust PfMO at osd.pentagon.dod-cio.mbx.zero-trust-portfolio-management-office@mail.mil if you require access to classified, FOUO, or CUI documents marked with an asterisk*

APPENDIX F: Acronyms / Definitions

Table 3. Acronyms

Acronym	Description
AI	Artificial Intelligence
BES	Budget Estimate Submission
C2C	Comply-to-Connect
C4I	Command, Control, Communications, Computers and Intelligence
CAPE	Office of Cost Assessment & Program Evaluation
CIO	Chief Information Officer
COA	Course of Action
CPG	DoD CIO Capability Programming Guidance
DAAS	Data, Applications, Assets, and Services
DAFAs	Defense Agencies and Field Activities
DA&M	Director, Administration and Management
DIB	Defense Industrial Base
DoD IE	Department of Defense Information Enterprise
DODIN	DoD Information Network
DOTmLPF-P	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy
DPG	Defense Planning Guidance
FYDP	Future Years Defense Program
JADC2	Joint All Domain Command and Control
JFHQ-DODIN	Joint Force Headquarters – Defense Information Networks
JWC	Joint Warfighting Concept
MILDEP	Military Department
MPE	Mission Partner Environment
NDAA	National Defense Authorization Act
NIPRNet	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NPE	Non-person Entity
NSS	National Security Systems
OT&E	Operational Test & Evaluation
PfMO	Portfolio Management Office
POM	Program Objective Memorandum
PPBE	Planning, Programming, Budgeting & Execution
SIPRNet	Secret Internet Protocol Router Network
SMART	Specific, Measurable, Achievable, Relevant, and Time-bound
ZT	Zero Trust
ZT RA	Zero Trust Reference Architecture

Table 4. Key Definitions

Term	Definition
DoD Advanced Zero Trust	Achievement of the full set of identified Zero Trust capability outcomes and activities that enable adaptive responses to cybersecurity risk and threats. Reaching an "advanced" state does not mean an end to maturing ZT; rather, protection of attack surfaces will continue to adapt and refine as the adversary's attack approaches and vectors mutate.
DoD Zero Trust Pillars	Seven capability pillars of Zero Trust that provide the foundational areas for the DoD Zero Trust Security Model and DoD ZT Architectures, including focus for the implementation of ZT controls (as defined by the *DoD Zero Trust Reference Architecture, v2*).
DoD Zero Trust Capability Roadmap	Lays out how the Department currently envisions achieving capability-based outcomes. The *Roadmap* defines ZT capability outcomes to achieve DoD Zero Trust Target Level, identifies activities, outlines dependencies and interdependencies impacting sequence and parallel development, and provides a general timeline to achieve outcomes by fiscal year.
DoD Zero Trust Ecosystem	Consists of the breadth of DoD leaders, mission owners, and partners (internal and external) who are stakeholders in the success of Zero Trust implemented across the Information Enterprise (IE).
DoD Zero Trust DOTmLPF-P Execution Enablers	Cross-cutting, non-technical capabilities and activities that address culture, governance, and elements of DOTmLPF-P (e.g., ZT Training, etc.) that support the design, development and deployment of the ZT Capabilities required to achieve the DoD Target and Advanced Levels.
DoD Zero Trust Framework	An official cybersecurity blueprint, based on the seven DoD Zero Trust Capability Pillars, which describes how the Department will achieve ZT by providing the foundation and the direction to help align on-going and future ZT-related efforts, investments and initiatives.
DoD Zero Trust Maturity Model	Depiction of the logical progression of an as-is security model to an advanced Zero Trust architecture as defined by the *DoD Zero Trust Reference Architecture, v2*.
DoD Zero Trust Portfolio Management Office	The Organization within the Office of the DoD CIO (CS) responsible for providing strategic guidance, directing alignment of efforts, and prioritizing resources to accelerate Zero Trust adoption and implementation across the DoD.
DoD Zero Trust Security Model	A more robust cybersecurity model that eliminates the idea of trusted or untrusted networks, devices, personas, or processes, and shifts to multi-attribute-based confidence levels that enable authentication and authorization policies based on the concept of least privileged access (as defined by the *DoD Zero Trust Reference Architecture, v2*).
DoD Zero Trust Target Level	The required minimum set of Zero Trust capability outcomes and activities necessary to secure and protect the Department's DAAS to manage risks from currently known threats; includes basic and intermediate Zero Trust maturity as defined by the ZT RA.