TLP:CLEAR

Zero Trust Maturity Model

April 2023

Version 2.0

Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

Disclaimer: This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp/.

Revision History

The version number will be updated as the document is modified. This document will be updated as needed to reflect modern security practices and technologies. Table 1 presents the document revision history.

Table 1: Revision History

Version	Date	Revision Description	Sections/Pages Affected
1.0	August 2021	Initial Release	All
2.0	April 2023*	Response to RFC Feedback	All

*Updated for release date

Zero Trust Maturity Model

Table of Contents

List of Figures

List of Tables

1. Introduction

The Cybersecurity and Infrastructure Security Agency (CISA) leads the nation's effort to understand, manage, and reduce cybersecurity risk, including by supporting Federal Civilian Executive Branch agencies in evolving and operationalizing cybersecurity programs and capabilities. CISA's Zero Trust Maturity Model (ZTMM) provides an approach to achieve continued modernization efforts related to zero trust within a rapidly evolving environment and technology landscape. This ZTMM is one of many paths that an organization can take in designing and implementing their transition plan to zero trust architectures in accordance with Executive Order (EO) 14028 "Improving the Nation's Cybersecurity" § (3)(b)(ii),[1] which requires that agencies develop a plan to implement a Zero Trust Architecture (ZTA). While the ZTMM is specifically tailored for federal agencies as required by EO 14028, all organizations should review and consider adoption of the approaches outlined in this document.

2. Current Environment

Recent cyber incidents[2,3] have highlighted the broad challenges of ensuring effective cybersecurity across the federal government, as with many large enterprises, and demonstrate that "business as usual" approaches are no longer sufficient to defend the nation from cyber threats. In leading the national effort to understand, manage, and reduce cyber risks, CISA must meet new challenges to safeguard the federal civilian executive branch using a clear, actionable, and risk-informed approach. Adequate cyber defense against emerging threats requires increased speed and agility to outpace adversaries by substantially increasing costs to threat actors and improving durability and resiliency to quickly recover to full operational capability.

CISA's cybersecurity mission is to defend and secure cyberspace by leading national efforts to drive and enable effective national cyber defense, enhance resilience of national critical functions, and advance a robust technology ecosystem. CISA plays a critical role in maintaining cyber situational awareness across FCEB agencies; securing the .gov domain; and aiding federal civilian agencies, critical infrastructure owners and operators, as well as industry partners in managing major cyber incidents. While CISA maintains capabilities to defend against and mitigate known or suspected cyber threats, an evolving threat landscape and the adoption of new and emerging technologies pose challenges.

EO 14028 marked a renewed commitment to and prioritization of federal cybersecurity modernization. Among other policy mandates, EO 14028 embraced zero trust as the desired security model for the federal government and called for FCEB agencies to develop plans to implement ZTAs. A typical plan will assess an agency's current cybersecurity state and plan for a fully implemented ZTA. As the lead agency on federal cybersecurity and risk reduction, CISA's ZTMM assists agencies in development of their zero trust strategies and continued evolution of their implementation plans and presents ways in which various CISA services can support zero trust solutions across agencies.

[1] Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 17, 2021). https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf.

[2] DHS CISA. *Emergency Directive 21-01- Mitigate SolarWinds Orion Code Compromise*. https://www.cisa.gov/emergency-directive-21-01.

[3] DHS CISA. *Emergency Directive 21-02 - Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*. https://www.cisa.gov/emergency-directive-21-02.

OMB Memorandum M-22-09, “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,”[4] detailed specific actions for federal agencies to adopt in alignment with the pillars outlined in the ZTMM. This memorandum sets forth a Federal ZTA strategy, requiring agencies to meet cybersecurity objectives by the end of Fiscal Year (FY) 2024 to reinforce FCEB defense. CISA revised the ZTMM to further align with M-22-09’s direction for agencies. FCEB agencies should review this memo in parallel with developing and implementing their zero trust strategies.

3. What Is Zero Trust?

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 provides the following zero trust and ZTA operative definition:

> **Zero trust** provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. **ZTA** is an enterprise’s cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZTA plan.[5]

SP 800-207 emphasizes that the goal of ZT is to “prevent unauthorized access to data and services coupled with making the access control enforcement as granular as possible.” Similarly, the National Security Telecommunications Advisory Committee (NSTAC) describes Zero Trust as “a cybersecurity strategy premised on the idea that no user or asset is to be implicitly trusted. It assumes that a breach has already occurred or will occur, and therefore, a user should not be granted access to sensitive information by a single verification done at the enterprise perimeter. Instead, each user, device, application, and transaction must be continually verified.”[6] Zero trust presents a shift from a location-centric model to an identity, context, and data-centric approach with fine-grained security controls between users, systems, applications, data, and assets that change over time; for these reasons, adopting a ZTA is a non-trivial effort. This shift provides the visibility needed to support the development, implementation, enforcement, and evolution of security policies. Fundamentally, zero trust may require a change in an organization’s cybersecurity philosophy and culture.

> The path to zero trust is an incremental process that may take years to implement.

Initially, the implementation of required capabilities and services will often lead to additional costs; however, in the long-term, zero trust will enable a more prudent allocation of security investments toward

[4] OMB Memo M-22-09. *Moving the U.S. Government Towards Zero Trust Cybersecurity Principles*. January 26, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[5] NIST SP 800-207: Zero Trust Architecture. 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

[6] The President’s National Security Telecommunications Advisory Committee. Report to the President on Zero Trust and Identity Management. February 2022. https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management.pdf.

the most critical data and services, rather than "one size fits all" security investments across the entire enterprise.

4. Challenges in Zero Trust Adoption

The Federal Government, as with most large enterprises, faces several challenges in implementing ZTA. Legacy systems often rely on "implicit trust," in which access and authorization are infrequently assessed based on fixed attributes; this conflicts with the core principle of adaptive evaluation of trust within a ZTA. Existing infrastructures built on implicit trust will require investment to change systems to better align with zero trust principles. Furthermore, as the technology landscape continues to evolve, new solutions and continued discussions on how to best achieve zero trust objectives are paramount.

Zero trust adoption requires engagement and cooperation from senior leadership, IT staff, data and system owners, and users across the Federal Government to effectively achieve design objectives and improve cybersecurity posture. Modernization of the Federal Government's cybersecurity will require agencies to transition stove-piped and siloed IT services and staff to coordinated and collaborative components of a zero trust strategy, with agency-wide buy in for a common architecture and governance policies. This includes current and future plans to adopt cloud technologies.[7]

Federal agencies are beginning their journeys to zero trust from different starting points. Some agencies may be further along or better positioned to make these advancements than others; however, regardless of starting point, successful zero trust adoption can produce numerous benefits such as improved productivity, enhanced end-user experiences, reduced IT costs, flexible access, and bolstered security.

5. Zero Trust Maturity Model

The ZTMM represents a gradient of implementation across five distinct pillars, in which minor advancements can be made over time toward optimization. The pillars, depicted in Figure 1, include **Identity**, **Devices**, **Networks**, **Applications and Workloads**, and **Data**. Each pillar includes general details regarding the following cross-cutting capabilities: *Visibility and Analytics*, *Automation and Orchestration*, and *Governance*.

[7] Agencies should review CISA's, United States Digital Services', and FedRAMP's jointly authored Cloud Security Technical Reference Architecture for additional guidance on recommend approaches to cloud migration and data protection. Cloud Security Technical Reference Architecture v.2 (cisa.gov).

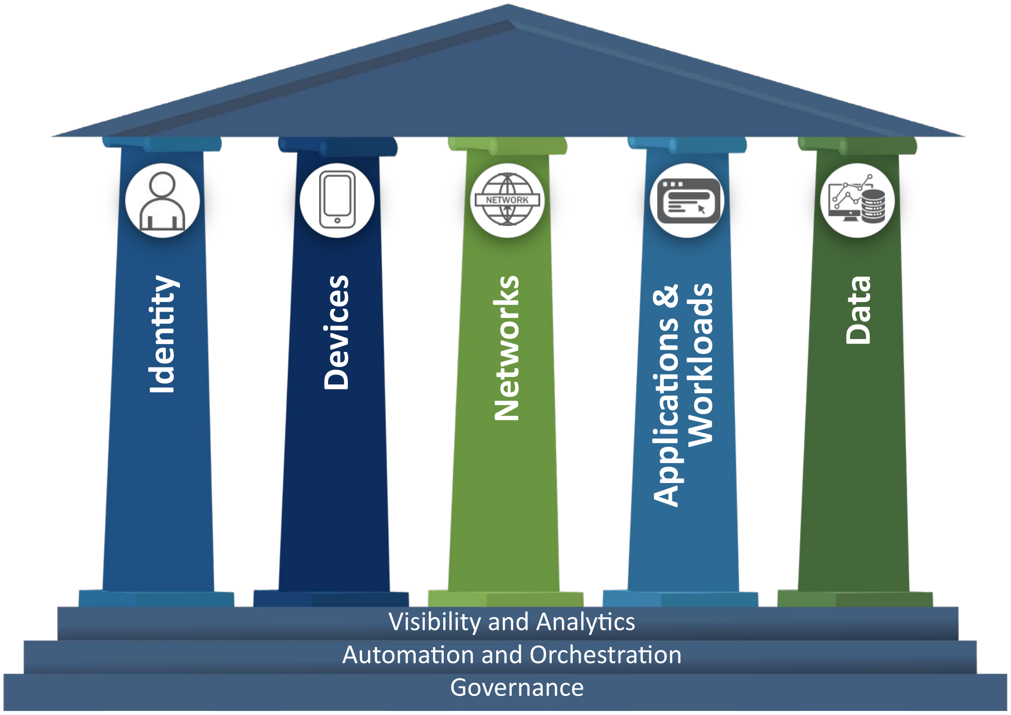


Figure 1: Zero Trust Maturity Model Pillars[8]

CISA's ZTMM is one of many paths to support the transition to zero trust.

Various ZTA publications informed the development of this maturity model (see Section 6 for additional details). This model reflects the seven tenets of zero trust as outlined in NIST SP 800-207:

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.

As agencies transition towards optimal zero trust implementations, associated solutions increasingly rely upon automated processes and systems that more fully integrate across pillars and more dynamically enforce policy decisions. Each pillar can progress at its own pace and may progress more quickly than others until cross-pillar coordination is required. However, this coordination can only be achieved with capabilities and dependencies compatible with one another and the enterprise-wide environment. This

[8] This illustration was inspired by Figure 1 of the American Council for Technology (ACT) and Industry Advisory Council (IAC) "Zero Trust Cybersecurity Current Trends," (2019). https://www.actiac.org/system/files/ACT-IAC%20Zero%20Trust%20Project%20Report%2004182019.pdf.

allows for and defines a gradual evolution to zero trust, distributing costs over time rather than entirely upfront.

In alignment with NIST's steps for transitioning to zero trust, agencies should assess their current enterprise systems, resources, infrastructure, personnel, and processes before investing in zero trust capabilities (including for the pillars and functions outlined in this model).[9] This assessment can assist agencies in identifying existing capabilities to support further zero trust maturity and gaps for prioritization. Agencies can also plan for opportunities to coordinate capabilities across the pillars to enable granular, least privilege access controls and mitigate additional risks. [10]

The three stages of the ZTM journey that advance from a Traditional starting point to Initial, Advanced, and Optimal will facilitate federal ZTA implementation. Each subsequent stage requires *greater* levels of protection, detail, and complexity for adoption.

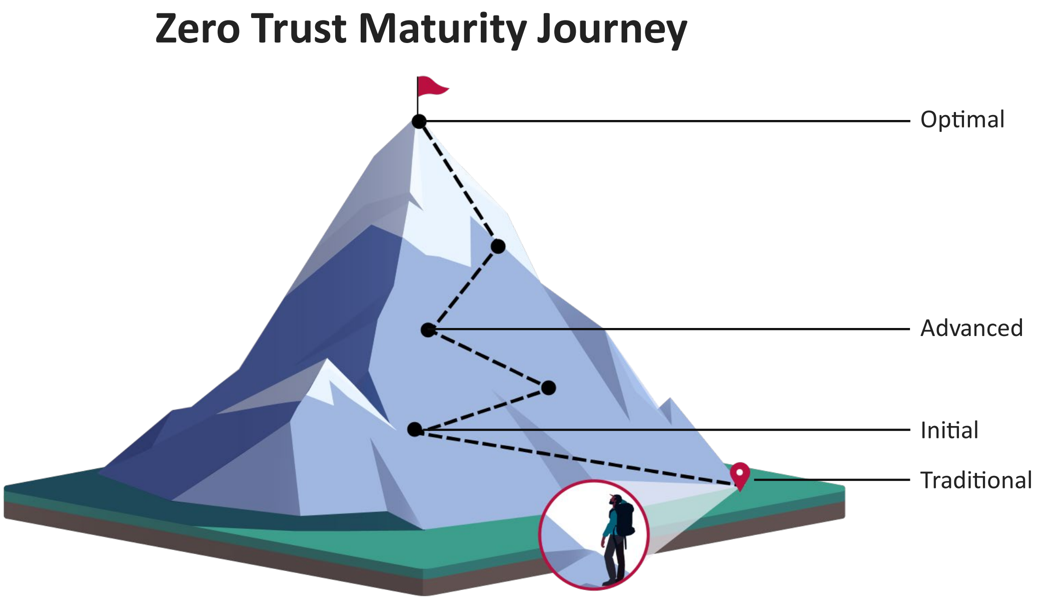


Figure 2: Zero Trust Maturity Journey

As seen in Figure 2, agencies should expect that required levels of effort and realized benefits will significantly increase as zero trust maturity progresses across and within pillars. As agencies chart their ZTA journey, they should explore opportunities to advance pillar maturity to align to specific mission needs and support further growth across other pillars. Figure 3 highlights the intended agency evolution over time from a traditional enterprise to a future state that features more dynamic updates, automated processes, integrated capabilities, and other characteristics of the Optimal stages (as described in the maturity model). These stages are dynamic and grow exponentially; planned progress from one maturity stage to another may shift in scope and impact over time.

[9] NIST White Paper. Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators. https://csrc.nist.gov/publications/detail/white-paper/2022/05/06/planning-for-a-zero-trust-architecture/final.

[10] See AC-6 in NIST SP 800-53 Revision 5. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

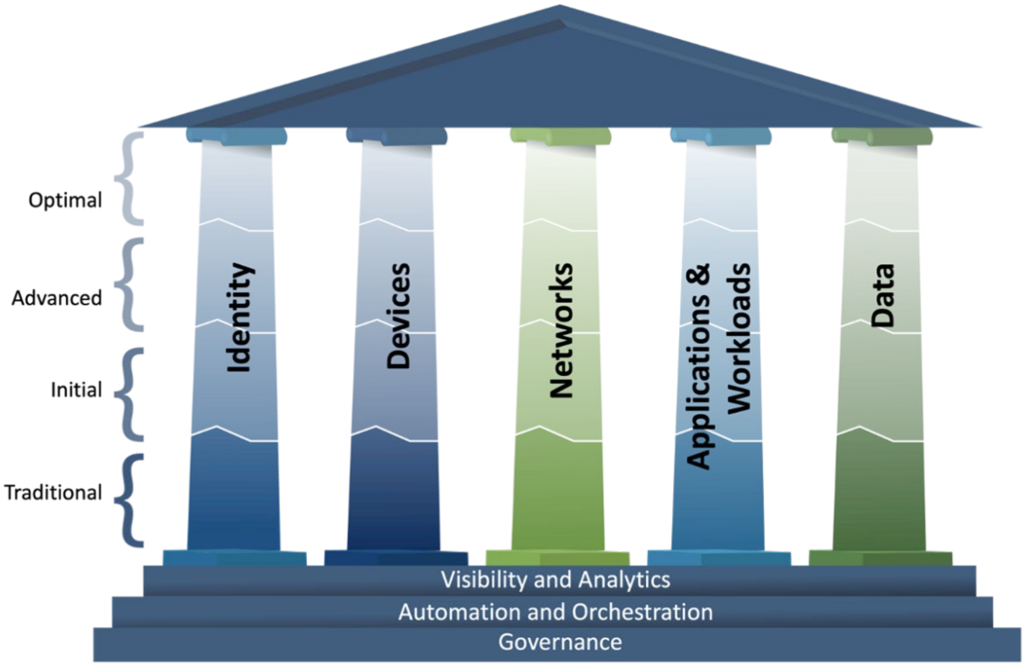
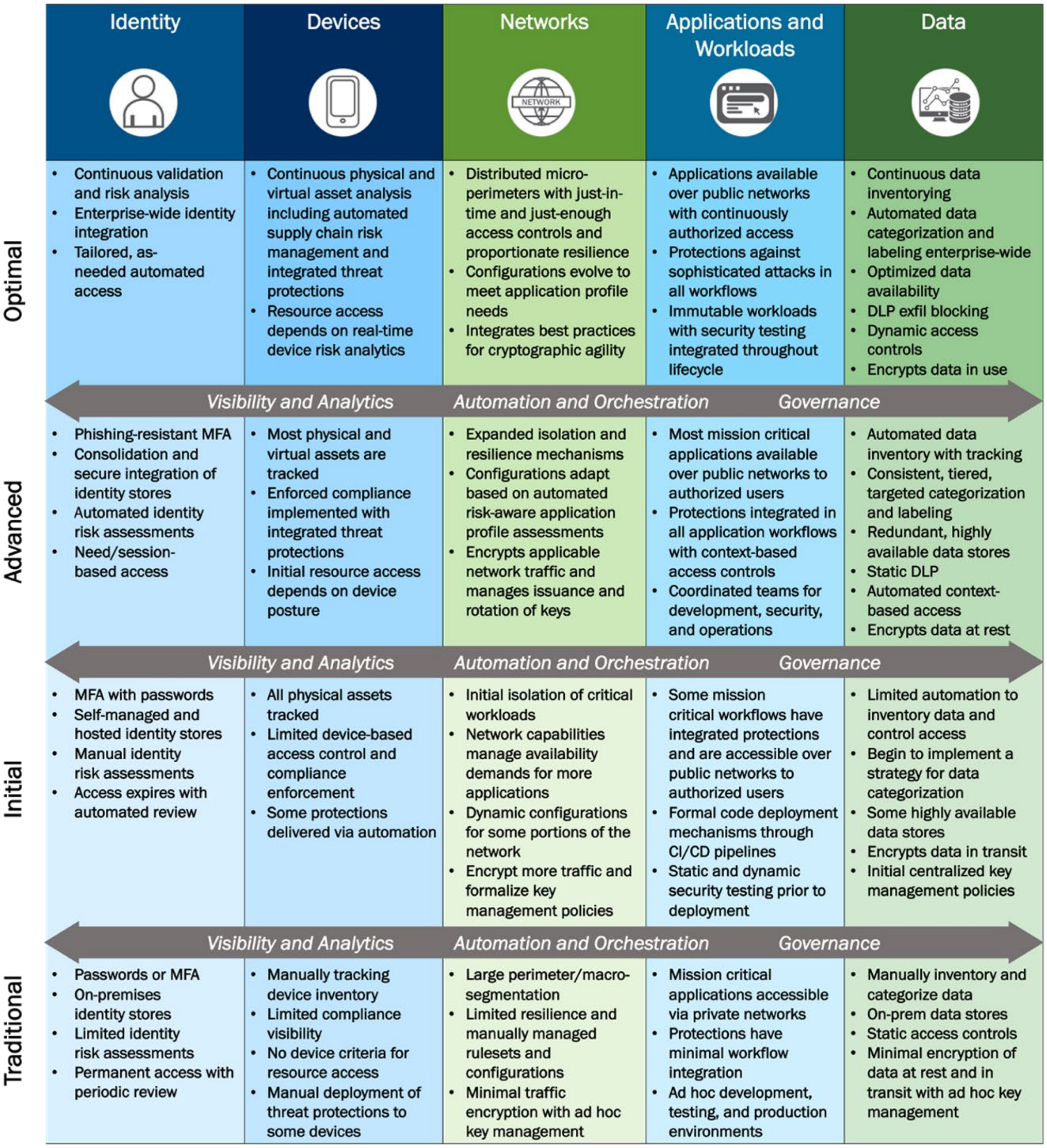


Figure 3: Zero Trust Maturity Evolution

Agencies should use the following guiding criteria of each stage to identify maturity for each zero trust technology pillar and provide consistency across the maturity model:

- **Traditional**—manually configured lifecycles (i.e., from establishment to decommissioning) and assignments of attributes (security and logging); static security policies and solutions that address one pillar at a time with discrete dependencies on external systems; least privilege established only at provisioning; siloed pillars of policy enforcement; manual response and mitigation deployment; and limited correlation of dependencies, logs, and telemetry.
- **Initial**—starting automation of attribute assignment and configuration of lifecycles, policy decisions and enforcement, and initial cross-pillar solutions with integration of external systems; some responsive changes to least privilege after provisioning; and aggregated visibility for internal systems.
- **Advanced**—wherever applicable, automated controls for lifecycle and assignment of configurations and policies with cross-pillar coordination; centralized visibility and identity control; policy enforcement integrated across pillars; response to pre-defined mitigations; changes to least privilege based on risk and posture assessments; and building toward enterprise-wide awareness (including externally hosted resources).
- **Optimal**—fully automated, just-in-time lifecycles and assignments of attributes to assets and resources that self-report with dynamic policies based on automated/observed triggers; dynamic least privilege access (just-enough and within thresholds) for assets and their respective dependencies enterprise-wide; cross-pillar interoperability with continuous monitoring; and centralized visibility with comprehensive situational awareness.

Figure 4 provides a high-level overview of the ZTMM, including key aspects of the pillar-specific functions for each pillar and across each maturity stage.



	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
	Visibility and Analytics		Automation and Orchestration		Governance
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
	Visibility and Analytics		Automation and Orchestration		Governance
Initial	• MFA with passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
	Visibility and Analytics		Automation and Orchestration		Governance
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

Figure 4: High-Level Zero Trust Maturity Model Overview

These maturity stages and the details associated with each pillar allow agencies to assess, plan, and maintain the investments needed to progress toward a ZTA. Subsections 0–5.5 provide high-level information to support agencies in transitioning to zero trust across the five different pillars: **Identity**, **Devices**, **Networks**, **Applications and Workloads**, and **Data**. Each pillar also includes general details regarding *Visibility and Analytics*, *Automation and Orchestration*, and *Governance* capabilities to support integration with that pillar and across the model.

These three cross-cutting capabilities highlight activities to support interoperability of functions across pillars based on the following descriptions:

- **Visibility and Analytics:** Visibility refers to the observable artifacts that result from the characteristics of and events within enterprise-wide environments.[11] The focus on cyber-related data analysis can help inform policy decisions, facilitate response activities, and build a risk profile to develop proactive security measures before an incident occurs.[12]
- **Automation and Orchestration:** Zero trust makes full use of automated tools and workflows that support security response functions across products and services while maintaining oversight, security, and interaction of the development process for such functions, products, and services.
- **Governance:** Governance refers to the definition and associated enforcement of agency cybersecurity policies, procedures, and processes, within and across pillars, to manage an agency's enterprise and mitigate security risks in support of zero trust principles and fulfillment of federal requirements.[13]

While the ZTMM covers many aspects of cybersecurity critical to federal enterprises, it does not address other aspects of cybersecurity such as activities related to incident response, specifics for logging, monitoring, alerting, forensic analysis, risk acceptance, recovery.[14] Other aspects of and best practices for enterprise cybersecurity posture management are not explicitly included within the maturity model functions. Although the maturity model is not intended to be exclusionary, it does not address challenges specific to operational technologies,[15] certain classes of internet of things (IoT) devices,[16] or broadly incorporating emerging technologies such as deception platforms, authenticated web application firewalls, behavior analytics, etc. Methodologies such as recommendations to best incorporate machine learning and artificial intelligence capabilities within zero trust solutions are not included in this model. Mature Agencies should take steps to monitor and assess the performance and integrity of their security capabilities, underlying infrastructure, and policies to detect unauthorized access and changes as they mature each pillar. Agencies should be careful to not create new opportunities for exploitation or weaken security protocols. Research and development are required to effectively assure software and hardware systems integrity at scale across federal enterprises.[17,18,19]

[11] See CISA's extensible Visibility Reference Framework (eVRF) Guidebook: https://www.cisa.gov/blog/2022/04/19/scuba-it-means-better-visibility-standards-and-security-practices-government-cloud.

[12] Agencies should review OMB Memo M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021) for further guidance on logging requirements as they make decisions and investments for visibility needs. https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf.

[13] Based on the Governance function of the Identify category of the NIST Cyber Security Framework Version 1.1: https://www.nist.gov/cyberframework/framework.

[14] Backups are included within the Data Pillar; however, for detailed guidance on data integrity and recovery, Agencies should consult NIST SP 1800-11: https://csrc.nist.gov/News/2020/sp-1800-11-data-integrity-ransomware-recovery.

[15] NIST. Guide to Operational Technology Security: NIST Requests Comments on Draft SP 800-82r3. April 2022. https://csrc.nist.gov/News/2022/guide-to-operational-technology-ot-security.

[16] NIST. Cybersecurity for IoT Program. https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program.

[17] NIST NCCOE: Supply Chain Assurance. https://www.nccoe.nist.gov/supply-chain-assurance.

[18] NIST NCCOE: Software Supply Chain and DevOps Security Practices. https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices.

[19] Agencies should review the information and resources available for Software Bill of Materials (SBOM) and Vulnerability Exploitability eXchange (VEX) as community advancements continue at: https://www.cisa.gov/sbom.

When planning ZTA implementation, agencies should make decisions based on factors which include risk, mission, federal requirements, and operating constraints. While this model is generally aligned to a federal enterprise's single administrative domain or accreditation boundary, agencies should also assess how their interactions with and reliance upon external partners, stakeholders, and service providers factor into their ZTA.[20] This maturity model should not be viewed as a strict set of requirements but as a general guide to help agencies successfully implement their ZTA and adopt an overall improved cybersecurity posture.

[20] These considerations span pillars and functions such as trusting credentials, assessing supply chains, differences in data categorization, policy exceptions, variations in risk thresholds, and more.

5.1 Identity

An identity refers to an attribute or set of attributes that uniquely describes an agency user or entity, including non-person entities.

Agencies should ensure and enforce user and entity access to the right resources at the right time for the right purpose without granting excessive access. Agencies should integrate identity, credential, and access management solutions where possible throughout their enterprise to enforce strong authentication, grant tailored context-based authorization, and assess identity risk for agency users and entities. Agencies should integrate their identity stores and management systems, where appropriate, to enhance awareness of enterprise identities and their associated responsibilities and authorities.

Table 2 lists identity functions pertaining to zero trust and considerations for Visibility and Analytics, Automation and Orchestration, and Governance within the context of identity.

Table 2: Identity Pillar

Function	Traditional	Initial	Advanced	Optimal
Authentication	Agency authenticates identity using either passwords or multi-factor authentication[21] (MFA) with static access for entity identity.	Agency authenticates identity using MFA, which may include passwords as one factor and requires validation of multiple entity attributes (e.g., locale or activity).	Agency begins to authenticate all identity using phishing-resistant MFA and attributes, including initial implementation of password-	Agency continuously validates identity with phishing-resistant MFA, not just when access is initially granted.

[21] CISA resources for MFA available at: https://www.cisa.gov/mfa.

Function	Traditional	Initial	Advanced	Optimal
			less MFA via FIDO2[22] or PIV[23].	
Identity Stores	Agency only uses self-managed, on-premises (i.e., planned, deployed, and maintained by agency) identity stores.	Agency has a combination of self-managed identity stores and hosted identity store(s) (e.g., cloud or other agency) with minimal integration between the store(s) (e.g., Single Sign-on.).	Agency begins to securely consolidate and integrate some self-managed and hosted identity stores.	Agency securely integrates their identity stores across all partners and environments as appropriate.
Risk Assessments	Agency makes limited determinations for identity risk (i.e., likelihood that an identity is compromised).	Agency determines identity risk using manual methods and static rules to support visibility.	Agency determines identity risk with some automated analysis and dynamic rules to inform access decisions and response activities.	Agency determines identity risk in real time based on continuous analysis and dynamic rules to deliver ongoing protection.
Access Management (New Function)	Agency authorizes permanent access with periodic review for both privileged and unprivileged accounts.	Agency authorizes access, including for privileged access requests, that expires with automated review.	Agency authorizes need-based and session-based access, including for privileged access request, that is tailored to actions and resources.	Agency uses automation to authorize just-in-time and just-enough access tailored to individual actions and individual resource needs.

[22] FIDO2 is a set of protocols developed in collaboration by the Fast IDentity Online (FIDO) Alliance and World Wide Web Consortium (W3C). FIDO2 is designed to enable easy, secure, and passwordless authentication. This approach leverages W3C's WebAuthn protocol and the FIDO Alliance's Client to Authenticator Protocol (CTAP) protocol.

FIDO Alliance. *FIDO Alliance - Open Authentication Standards More Secure than Passwords*. https://fidoalliance.org/.

World Wide Web Consortium. *Web Authentication: An API for accessing Public Key Credentials.* https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.

FIDO Alliance. Client to Authenticator Protocol. Proposed Standard, June 2021. https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-errata-20220621.html.

[23] Personal Identity Verification. A PIV credential is a U.S. federal government-wide credential used to access federally controlled facilities and information systems at the appropriate security level. https://playbooks.idmanagement.gov/piv/.

Function	Traditional	Initial	Advanced	Optimal
Visibility and Analytics Capability	Agency collects user and entity activity logs, especially for privileged credentials, and performs some routine manual analysis.	Agency collects user and entity activity logs and performs routine manual analysis and some automated analysis, with limited correlation between log types.	Agency performs automated analysis across some user and entity activity log types and augments collection to address gaps in visibility.	Agency maintains comprehensive visibility and situational awareness across enterprise by performing automated analysis over user activity log types, including behavior-based analytics.
Automation and Orchestration Capability	Agency manually orchestrates (onboards, offboards, and disables) self-managed identities (users and entities), with little integration, and performs regular review.	Agency manually orchestrates privileged and external identities and automates orchestration of non-privileged users and of self-managed entities.	Agency manually orchestrates privileged user identities and automates orchestration of all identities with integration across all environments.	Agency automates orchestration of all identities with full integration across all environments based on behaviors, enrollments, and deployment needs.
Governance Capability	Agency implements identity policies (authentication, credentials, access, lifecycle, etc.) with enforcement via static technical mechanisms and manual review.	Agency defines and begins implementing identity policies for enterprise-wide enforcement with minimal automation and manual updates.	Agency implements identity policies for enterprise-wide enforcement with automation and updates policies periodically.	Agency implements and fully automates enterprise-wide identity policies for all users and entities across all systems with continuous enforcement and dynamic updates.

5.2 Devices

A device refers to any asset (including its hardware, software, firmware, etc.) that can connect to a network, including servers, desktop and laptop machines, printers, mobile phones, IoT devices, networking equipment, and more.

Devices may be agency-owned or bring-your-own-device (BYOD) property of employees, partners, or visitors. Agencies should secure all agency devices, manage the risks of authorized devices that are not agency-controlled, and prevent unauthorized devices from accessing resources. Device management includes maintaining a dynamic inventory of all assets including their hardware, software, firmware, etc., along with their configurations and associated vulnerabilities as they become known.

Many devices present specific ZTA challenges and must be evaluated on a case-by-case basis as part of a risk-based process. For example, networking equipment, printers, and others may offer limited options for authentication, visibility, and security. Agencies employing BYOD policies will likely have fewer options to maintain visibility and control of such devices. The technological landscape for devices continues to change and as agencies incorporate additional devices into their enterprise, they will need to continue to manage the evolving risks associated with these devices.[24] In some cases, agencies may be unable to adopt the guidance for certain subsets of their devices. Agencies will also face challenges in ensuring trusted devices and their services have not reached end-of-life and are still covered by their life-time-support, as legacy devices often have a higher number of unmitigated vulnerabilities, available misconfigurations, and unknown risks. However, despite these challenges, agencies should still be able to make considerable progress toward a ZTA.

On-premises computing asset management involves documenting and managing physical assets (devices). As agencies move to cloud environments, this creates new considerations and opportunities for managing and tracking agency cloud and virtual assets. Cloud assets include compute resources (e.g., virtual machines, servers, or containers), storage resources (e.g., block storage or file storage), platform assets (e.g., databases, web servers, message buses/queues), and network resources (e.g., virtual networks, VPNs, gateways, DNS services, etc.) and virtual resources associated with other managed cloud services (e.g., artificial intelligence models).

Table 3 lists functions for devices pertaining to zero trust, as well as considerations for *Visibility and Analytics*, *Automation and Orchestration*, and *Governance* within the context of devices.

[24] Agencies should consult OMB Memo M-22-01 *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*. October 8, 2021. https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf.

Table 3: Devices Pillar

Function	Traditional	Initial	Advanced	Optimal
Policy Enforcement & Compliance Monitoring (New Function)	Agency has limited, if any, visibility (i.e., ability to inspect device behavior) into device compliance with few methods of enforcing policies or managing software, configurations, or vulnerabilities.	Agency receives self-reported device characteristics (e.g., keys, tokens, users, etc., on the device) but has limited enforcement mechanisms. Agency has a preliminary, basic process in place to approve software use and push updates and configuration changes to devices.	Agency has verified insights (i.e., an administrator can inspect and verify the data on device) on initial access to device and enforces compliance for most devices and virtual assets. Agency uses automated methods to manage devices and virtual assets, approve software, and identify vulnerabilities and install patches.	Agency continuously verifies insights and enforces compliance throughout the lifetime of devices and virtual assets. Agency integrates device, software, configuration, and vulnerability management across all agency environments, including for virtual assets.
Asset & Supply Chain Risk Management (New Function)	Agency does not track physical or virtual assets in an enterprise-wide or cross-vendor manner and manages its own supply chain acquisition of devices and services in ad hoc fashion with a limited view of enterprise risks.	Agency tracks all physical and some virtual assets and manages supply chain risks by establishing policies and control baselines according to federal recommendations using a robust framework, (e.g., NIST SCRM.)[25]	Agency begins to develop a comprehensive enterprise view of physical and virtual assets via automated processes that can function across multiple vendors to verify acquisitions, track development cycles, and provide third-party assessments.	Agency has a comprehensive, at- or near-real-time view of all assets across vendors and service providers, automates its supply chain risk management as applicable, builds operations that tolerate supply chain failures, and incorporates best practices.
Resource Access (Formerly Data Access)	Agency does not require visibility into devices or virtual assets used to access resources.	Agency requires some devices or virtual assets to report characteristics then use this information to approve resource access.	Agency's initial resource access considers verified device or virtual asset insights.	Agency's resource access considers real-time risk analytics within devices and virtual assets.

[25] NIST. NIST Updates Cybersecurity Guidance for Supply Chain Risk Management. May 5, 2022. https://www.nist.gov/news-events/news/2022/05/nist-updates-cybersecurity-guidance-supply-chain-risk-management.

Function	Traditional	Initial	Advanced	Optimal
Device Threat Protection (New Function)	Agency manually deploys threat protection capabilities to some devices.	Agency has some automated processes for deploying and updating threat protection capabilities to devices and to virtual assets with limited policy enforcement and compliance monitoring integration.	Agency begins to consolidate threat protection capabilities to centralized solutions for devices and virtual assets and integrates most of these capabilities with policy enforcement and compliance monitoring.	Agency has a centralized threat protection security solution(s) deployed with advanced capabilities for all devices and virtual assets and a unified approach for device threat protection, policy enforcement, and compliance monitoring.
Visibility and Analytics Capability	Agency uses a physically labeled inventory and limited software monitoring to review devices on a regular basis with some manual analysis.	Agency uses digital identifiers (e.g., interface addresses, digital tags) alongside a manual inventory and endpoint monitoring of devices when available. Some agency devices and virtual assets are under automated analysis (e.g., software-based scanning) for anomaly detection based on risk.	Agency automates both inventory collection (including endpoint monitoring on all standard user devices, e.g., desktops and laptops, mobile phones, tablets, and their virtual assets) and anomaly detection to detect unauthorized devices.	Agency automates status collection of all network-connected devices and virtual assets while correlating with identities, conducting endpoint monitoring, and performing anomaly detection to inform resource access. Agency tracks patterns of provisioning and/or de-provisioning of virtual assets for anomalies.
Automation and Orchestration Capability	Agency manually provisions, configures, and/or registers devices within the enterprise.	Agency begins to use tools and scripts to automate the process of provisioning, configuration, registration, and/or deprovisioning for devices and virtual assets.	Agency has implemented monitoring and enforcement mechanisms to identify and manually disconnect or isolate non-compliant (vulnerable, unverified certificate; unregistered mac address) devices and virtual assets.	Agency has fully automated processes for provisioning, registering, monitoring, isolating, remediating, and deprovisioning devices and virtual assets.

Function	Traditional	Initial	Advanced	Optimal
Governance Capability	Agency sets some policies for the lifecycle[26] of their traditional and peripheral computing devices and relies on manual processes to maintain (e.g., update, patch, sanitize) these devices.	Agency sets and enforces policies for the procurement of new devices, the lifecycle of non-traditional computing devices and virtual assets, and for regularly conducting monitoring and scanning of devices.	Agency sets enterprise-wide policies for the lifecycle of devices and virtual assets, including their enumeration and accountability, with some automated enforcement mechanisms.	Agency automates policies for the lifecycle of all network-connected devices and virtual assets across the enterprise.

[26] Lifecycle includes procuring, configuring, tracking, monitoring, updating, using, sanitizing, deprovisioning, and recovering devices.

5.3 Networks

A network refers to an open communications medium including typical channels such as agency internal networks, wireless networks, and the Internet as well as other potential channels such as cellular and application-level channels used to transport messages.

ZTAs enable a shift away from traditional perimeter-focused approaches to security and permit agencies to manage internal and external traffic flows, isolate hosts, enforce encryption, segment activity, and enhance enterprise-wide network visibility. ZTAs permit security controls to be implemented closer to the applications, data, and other resources and augment traditional network-based protections and improve defense-in-depth. Each application can be treated uniquely by the network for its demands on access, priority, reachability, connections to dependency services, and connection pathways. These network application demands can be captured as an application profile, and repeated profiles can then be treated as a traffic class.

Table 4 lists network functions pertaining to zero trust and the considerations for *Visibility and Analytics*, *Automation and Orchestration*, and *Governance* within the context of networks.

Table 4: Networks Pillar

Function	Traditional	Initial	Advanced	Optimal
Network Segmentation	Agency defines their network architecture using large perimeter/macro-segmentation with minimal restrictions on reachability within network segments. Agency may also rely on multi-service interconnections (e.g., bulk traffic VPN tunnels).	Agency begins to deploy network architecture with the isolation of critical workloads, constraining connectivity to least function principles, and a transition toward service-specific interconnections.	Agency expands deployment of endpoint and application profile isolation mechanisms to more of their network architecture with ingress/egress micro-perimeters and service-specific interconnections.	Agency network architecture consists of fully distributed ingress/egress micro-perimeters and extensive micro-segmentation based around application profiles with dynamic just-in-time and just-enough connectivity for service-specific interconnections.
Network Traffic Management (New Function)	Agency manually implements static network rules and configurations to manage traffic at service provisioning, with limited monitoring capabilities (e.g.,	Agency establishes application profiles with distinct traffic management features and begins to map all applications to these profiles. Agency expands	Agency implements dynamic network rules and configurations for resource optimization that are periodically adapted based upon automated risk-aware	Agency implements dynamic network rules and configurations that continuously evolve to meet application profile needs and reprioritize applications

Function	Traditional	Initial	Advanced	Optimal
	application performance monitoring or anomaly detection) and manual audits and reviews of profile changes for mission critical applications.	application of static rules to all applications and performs periodic manual audits of application profile assessments.	and risk-responsive application profile assessments and monitoring.	based on mission criticality, risk, etc.
Traffic Encryption (Formerly Encryption)	Agency encrypts minimal traffic and relies on manual or ad hoc processes to manage and secure encryption keys.	Agency begins to encrypt all traffic to internal applications, to prefer encryption for traffic to external applications[27], to formalize key management policies, and to secure server/service encryption keys.	Agency ensures encryption for all applicable internal and external traffic protocols,[28] manages issuance and rotation of keys and certificates, and begins to incorporate best practices for cryptographic agility.[29]	Agency continues to encrypt traffic as appropriate, enforces least privilege principles for secure key management enterprise-wide, and incorporates best practices for cryptographic agility as widely as possible.
Network Resilience (New Function)	Agency configures network capabilities on a case-by-case basis to only match individual application availability demands with limited resilience mechanisms for workloads not deemed mission critical.	Agency begins to configure network capabilities to manage availability demands for additional applications and expand resilience mechanisms for workloads not deemed mission critical.	Agency has configured network capabilities to dynamically manage the availability demands and resilience mechanisms for the majority of their applications.	Agency integrates holistic delivery and awareness in adapting to changes in availability demands for all workloads and provides proportionate resilience.
Visibility and Analytics Capability	Agency incorporates limited boundary-focused network monitoring capabilities with	Agency employs network monitoring capabilities based on known indicators of	Agency deploys anomaly-based network detection capabilities to develop	Agency maintains visibility into communication across all agency networks and

[27] For example, when both HTTP and HTTPS options are available, policies and settings prefer HTTPS.

[28] There are a variety of resources agencies should review in regard to encrypting and decrypting network traffic (or not) for inspection and visibility needs as part of their zero trust adoption: OMB M-15-13, M-19-26, M-22-09, DHS Binding Operational Directive 18-01, NIST SP 800-207, among others. See also: https://www.cisa.gov/uscert/ncas/alerts/TA17-075A.

[29] DHS. Cryptographic Agility Infographic. May 12, 2022. https://www.dhs.gov/publication/cryptographic-agility-infographic.

Function	Traditional	Initial	Advanced	Optimal
	minimal analysis to start developing centralized situational awareness.	compromise (including network enumeration) to develop situational awareness in each environment and begins to correlate telemetry across traffic types and environments for analysis and threat hunting activities.	situational awareness across all environments, begins to correlate telemetry from multiple sources for analysis, and incorporates automated processes for robust threat hunting activities.	environments while enabling enterprise-wide situational awareness and advanced monitoring capabilities that automate telemetry correlation across all detection sources.
Automation and Orchestration Capability	Agency uses manual processes to manage the configuration and resource lifecycle for agency networks and environments with periodic integration of policy requirements and situational awareness.	Agency begins using automated methods to manage the configuration and resource lifecycle for some agency networks or environments and ensures that all resources have a defined lifetime based on policies and telemetry.	Agency uses automated change management methods (e.g., CI/CD) to manage the configuration and resource lifecycle for all agency networks and environments, responding to and enforcing policies and protections against perceived risks.	Agency networks and environments are defined using infrastructure-as-code managed by automated change management methods, including automated initiation and expiration to align with changing needs.
Governance Capability	Agency implements static network policies (access, protocols, segmentation, alerts, and remediation) with an approach focused on perimeter protections.	Agency defines and begins to implement policies tailored to individual network segments and resources while also inheriting corporate-wide rules as appropriate.	Agency incorporates automation in implementing tailored policies and facilitates the transition from perimeter-focused protections.	Agency implements enterprise-wide network policies that enable tailored, local controls; dynamic updates; and secure external connections based on application and user workflows.

5.4 Applications and Workloads

Applications and workloads include agency systems, computer programs, and services that execute on-premises, on mobile devices, and in cloud environments.

Agencies should manage and secure their deployed applications and should ensure secure application delivery. Granular access controls and integrated threat protections can offer enhanced situational awareness and mitigate application-specific threats. Per OMB M-22-09, agencies should begin to explore opportunities to make their applications available over public networks to authorized users. Best practices for DevSecOps and CI/CD processes, including the use of immutable workloads, should also be adopted to the extent possible.[30,31] Agencies should explore options to shift their operations away from a focus on accreditation boundaries and updating ATOs to supporting applications as if they are externally facing and provide commensurate security.

Table 5 lists application workload functions pertaining to zero trust, as well as the considerations for *Visibility and Analytics*, *Automation and Orchestration*, and *Governance* within the context of applications and workloads.

Table 5: Applications and Workloads

Function	Traditional	Initial	Advanced	Optimal
Application Access (Formerly Access Authorization)	Agency authorizes access to applications primarily based on local authorization and static attributes.	Agency begins to implement authorizing access capabilities to applications that incorporate contextual information (e.g., identity, device compliance, and/or other attributes) per request with expiration.	Agency automates application access decisions with expanded contextual information and enforced expiration conditions that adhere to least privilege principles.	Agency continuously authorizes application access, incorporating real-time risk analytics and factors such as behavior or usage patterns.
Application Threat Protections (Formerly Threat Protections)	Agency threat protections have minimal integration with application workflows, applying general purpose	Agency integrates threat protections into mission critical application workflows, applying	Agency integrates threat protections into all application workflows, protecting against some	Agency integrates advanced threat protections into all application workflows, offering real-time visibility

[30] NIST Projects: DevSecOps. https://csrc.nist.gov/Projects/devsecops#plans.

[31] NIST SP 800-204C: Implementation of DevSecOps for a Microservices-based Application with Service Mesh. March 8, 2022. https://csrc.nist.gov/publications/detail/sp/800-204c/final.

Function	Traditional	Initial	Advanced	Optimal
	protections for known threats.	protections against known threats and some application-specific threats.	application-specific and targeted threats.	and content-aware protections against sophisticated attacks tailored to applications.
Accessible Applications (Formerly Accessibility)	Agency makes some mission critical applications[32] available only over private networks and protected public network connections (e.g., VPN) with monitoring.	Agency makes some of their applicable mission critical applications available over open public networks to authorized users with need via brokered connections.	Agency makes most of their applicable mission critical applications available over open public network connections to authorized users as needed.	Agency makes all applicable applications available over open public networks to authorized users and devices, where appropriate, as needed.
Secure Application Development and Deployment Workflow (New Function)	Agency has ad hoc development, testing, and production environments with non-robust code deployment mechanisms.	Agency provides infrastructure for development, testing, and production environments (including automation) with formal code deployment mechanisms through CI/CD pipelines and requisite access controls in support of least privilege principles.	Agency uses distinct and coordinated teams for development, security, and operations while removing developer access to production environment for code deployment.	Agency leverages immutable workloads where feasible, only allowing changes to take effect through redeployment, and removes administrator access to deployment environments in favor of automated processes for code deployment.
Application Security Testing (Formerly Application Security)	Agency performs application security testing prior to deployment, primarily via manual testing methods.	Agency begins to use static and dynamic (i.e., application is executing) testing methods to perform security testing, including manual expert analysis, prior to application deployment.	Agency integrates application security testing into the application development and deployment process, including the use of periodic dynamic testing methods.	Agency integrates application security testing throughout the software development lifecycle across the enterprise with routine automated testing of deployed applications.

[32] This does not include National Security Systems. See National Security Memorandum (NSM)-8 “Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems.” https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/.

Function	Traditional	Initial	Advanced	Optimal
Visibility and Analytics Capability	Agency performs some performance and security monitoring of mission critical applications with limited aggregation and analytics.	Agency begins to automate application profile (e.g., state, health, and performance) and security monitoring for improved log collection, aggregation, and analytics.	Agency automates profile and security monitoring for most applications with heuristics to identify application-specific and enterprise-wide trends and refines processes over time to address gaps in visibility.	Agency performs continuous and dynamic monitoring across all applications to maintain enterprise-wide comprehensive visibility.
Automation and Orchestration Capability	Agency manually establishes static application hosting location and access at provisioning with limited maintenance and review.	Agency periodically modifies application configurations (including location and access) to meet relevant security and performance goals.	Agency automates application configurations to respond to operational and environmental changes.	Agency automates application configurations to continuously optimize for security and performance.
Governance Capability	Agency relies primarily on manual enforcement policies for application access, development, deployment, software asset management, security testing and evaluation (ST&E) at technology insertion, patching, and tracking software dependencies.	Agency begins to automate policy enforcement for application development (including access to development infrastructure), deployment, software asset management, ST&E at technology insertion, patching, and tracking software dependencies based upon mission needs (for example, with Software Bill of Materials).	Agency implements tiered, tailored policies enterprise-wide for applications and all aspects of the application development and deployment lifecycles and leverages automation, where possible, to support enforcement.	Agency fully automates policies governing applications development and deployment, including incorporating dynamic updates for applications through the CI/CD pipeline.

5.5 Data

Data includes all structured and unstructured files and fragments that reside or have resided in federal systems, devices, networks, applications, databases, infrastructure, and backups (including on-premises and virtual environments) as well as the associated metadata.

Agency data should be protected on devices, in applications, and on networks in accordance with federal requirements. Agencies should inventory, categorize, and label data;[33] protect data at rest and in transit; and deploy mechanisms to detect and stop data exfiltration. Agencies should carefully craft and review data governance policies to ensure all data lifecycle security aspects are appropriately enforced across the enterprise.

Table 6 lists data functions pertaining to zero trust, as well as the considerations for *Visibility and Analytics, Automation and Orchestration, and Governance* within the data context.

Table 6: Data

Function	Traditional	Initial	Advanced	Optimal
Data Inventory Management	Agency manually identifies and inventories some agency data (e.g., mission critical data).	Agency begins to automate data inventory processes for both on-premises and in cloud environments, covering most agency data, and begins to incorporate protections against data loss.	Agency automates data inventory and tracking enterprise-wide, covering all applicable agency data, with data loss prevention strategies based upon static attributes and/or labels.	Agency continuously inventories all applicable agency data and employs robust data loss prevention strategies that dynamically block suspected data exfiltration.
Data Categorization (New Function)	Agency employs limited and ad hoc data categorization capabilities.	Agency begins to implement a data categorization strategy with defined labels and manual enforcement mechanisms.	Agency automates some data categorization and labeling processes in a consistent, tiered, targeted manner with simple, structured formats and regular review.	Agency automates data categorization and labeling enterprise-wide with robust techniques; granular, structured formats; and mechanisms to address all data types.

[33] NIST NCCOE: Data Classification. https://www.nccoe.nist.gov/data-classification.

Function	Traditional	Initial	Advanced	Optimal
Data Availability (New Function)	Agency primarily makes data available from on-premises data stores with some off-site backups.	Agency makes some data available from redundant, highly available data stores (e.g., cloud) and maintains off-site backups for on-premises data.	Agency primarily makes data available from redundant, highly available data stores and ensures access to historical data.	Agency uses dynamic methods to optimize data availability, including historical data, according to user and entity need.
Data Access	Agency governs user and entity access (e.g., permissions to read, write, copy, grant others access, etc.) to data through static access controls.	Agency begins to deploy automated data access controls that incorporate elements of least privilege across the enterprise.	Agency automates data access controls that consider various attributes such as identity, device risk, application, data category, etc., and are time limited where applicable.	Agency automates dynamic just-in-time and just-enough data access controls enterprise-wide with continuous review of permissions.
Data Encryption	Agency encrypts minimal agency data at rest and in transit and relies on manual or ad hoc processes to manage and secure encryption keys.	Agency encrypts all data in transit and, where feasible, data at rest (e.g., mission critical data and data stored in external environments) and begins to formalize key management policies and secure encryption keys.[34]	Agency encrypts all data at rest and in transit across the enterprise to the maximum extent possible, begins to incorporate cryptographic agility, and protects encryption keys (i.e., secrets are not hard coded and are rotated on a regular basis).	Agency encrypts data in use where appropriate, enforces least privilege principles for secure key management enterprise-wide, and applies encryption using up-to-date standards and cryptographic agility to the extent possible.[35]
Visibility and Analytics Capability	Agency has limited visibility into data including location, access, and usage, with analysis consisting primarily of manual processes.	Agency obtains visibility based on data inventory management, categorization, encryption, and access attempts, with some	Agency maintains data visibility in a more comprehensive, enterprise-wide manner with automated analysis and correlation and	Agency has visibility across the full data lifecycle with robust analytics, including predictive analytics, that support comprehensive views of agency data and

[34] This should include efforts to consolidate key stores and reduce reliance on one-off or siloed key stores.

[35] See NIST for relevant standards and updates such as: (1) https://www.nist.gov/itl/fips-general-information, (2) https://www.nist.gov/cryptography, and (3) https://csrc.nist.gov/publications/detail/nistir/8413/final

Function	Traditional	Initial	Advanced	Optimal
		automated analysis and correlation.	begins to employ predictive analytics.	continuous security posture assessment.
Automation and Orchestration Capability	Agency implements data lifecycle and security policies (e.g., access, usage, storage, encryption, configurations, protections, backups, categorization, sanitization) through manual, and potentially ad hoc, processes.	Agency uses some automated processes to implement data lifecycle and security policies.	Agency implements data lifecycle and security policies primarily through automated methods for most agency data in a consistent, tiered, targeted manner across the enterprise.	Agency automates, to the maximum extent possible, data lifecycles and security policies for all agency data across the enterprise.
Governance Capability	Agency relies on ad hoc data governance policies (e.g., for protection, categorization, access, inventorying, storage, recovery, removal, etc.) with manual implementation.	Agency defines high-level data governance policies and relies primarily on manual, segmented implementation.	Agency begins integration of data lifecycle policy enforcement across the enterprise, enabling more unified definitions for data governance policies.	Agency data lifecycle policies are unified to the maximum extent possible and dynamically enforced across the enterprise.

5.6 Cross-Cutting Capabilities

The cross-cutting capabilities *Visibility and Analytics*, *Automation and Orchestration*, and *Governance* provide opportunities to integrate advancements across each of the five pillars. As agencies mature these capabilities with respect to a given pillar, they can also mature each capability independent of the pillars. *Visibility and Analytics* supports comprehensive visibility that informs policy decisions and facilitates response activities. *Automation and Orchestration* capabilities leverage these insights to support robust and streamlined operations to handle security incidents and respond to events as they arise. *Governance* enables agencies to manage and monitor their regulatory, legal, environmental, federal, and operational requirements in support of risk-based decision making. Governance capabilities also ensure the right people, process, and technology are in place to support mission, risk, and compliance objectives.

Table 7 provides a high-level maturity evolution for each of these cross-cutting capabilities.

Table 7: Cross-Cutting Capabilities

Function	Traditional	Initial	Advanced	Optimal
Visibility and Analytics	Agency manually collects limited logs across their enterprise with low fidelity and minimal analysis.	Agency begins to automate the collection and analysis of logs and events for mission critical functions and regularly assesses processes for gaps in visibility.	Agency expands the automated collection of logs and events enterprise-wide (including virtual environments) for centralized analysis that correlates across multiple sources.	Agency maintains comprehensive visibility enterprise-wide via centralized dynamic monitoring and advanced analysis of logs and events.
Automation and Orchestration	Agency relies on static and manual processes to orchestrate operations and response activities with limited automation.	Agency begins automating orchestration and response activities in support of critical mission functions.	Agency automates orchestration and response activities enterprise-wide, leveraging contextual information from multiple sources to inform decisions.	Agency orchestration and response activities dynamically respond to enterprise-wide changing requirements and environmental changes.
Governance	Agency implements policies in an ad hoc manner across the enterprise, with policies enforced via manual processes or static technical mechanisms.	Agency defines and begins implementing policies for enterprise-wide enforcement with minimal automation and manual updates.	Agency implements tiered, tailored policies enterprise-wide and leverages automation where possible to support enforcement. Access policy decisions incorporate	Agency implements and fully automates enterprise-wide policies that enable tailored local controls with continuous enforcement and dynamic updates.

Function	Traditional	Initial	Advanced	Optimal
			contextual information from multiple sources.	

6. References

CISA consulted the following Federal Government ZTA publications while developing and revising this guidance.

Office of Management and Budget M-22-09
This memorandum sets forth a Federal zero trust architecture strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defense against increasingly sophisticated and persistent threat campaigns. The strategy includes components that place significant emphasis on strong enterprise identity and access controls (including MFA), require encrypting all network traffic as soon as practicable, support building a foundation to automate security access rules, and treat every application as internet accessible.

National Institute of Standards and Technology Special Publication 800-207
NIST's SP 800-207 describes zero trust for enterprise security architects to aid understanding of zero trust for civilian unclassified systems and provides a road map to migrate and deploy zero trust security concepts to an enterprise environment. SP 800-207 is the product of a collaboration between multiple federal agencies and is overseen by the Federal Chief Information Officer (CIO) Council. NIST is developing and releasing additional ZTA implementation guidance.[36]

Department of Defense Zero Trust Reference Architecture
The Department of Defense (DoD)'s Zero Trust Reference Architecture describes data-centric enterprise standards and capabilities that can be used to successfully advance the DoD Information Network (DoDIN) into an interoperable zero trust end state. [37]

National Security Agency Embracing Zero Trust Security Model
The NSA's Embracing Zero Trust Security Model explains the benefits and implementation challenges of a zero trust security model. [38] It discusses the importance of building a detailed strategy, dedicating the necessary resources, maturing the implementation, and fully committing to the zero trust model to achieve the desired results. The document's recommendations will assist cybersecurity leaders, enterprise network owners, and administrators considering embracing this modern cybersecurity model.

7. CISA Resources

CISA programs provide cybersecurity support and guidance across the zero trust pillar areas, including the integration of the pillars into a ZTA. The following documents are useful resources for agencies migrating to zero trust. CISA will continue to review and refine these resources as agencies develop ZTAs and will add additional resources to the collection over time.

Continuous Diagnostics and Mitigation
CDM guidance can be found on the CDM homepage.

High Value Assets

[36] NIST. "Implementing a Zero Trust Architecture Project". https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture.

[37] DoD. "Zero Trust Reference Architecture". Version 2.0. July 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf.

[38] NSA. "Embracing a Zero Trust Security Model". Version 1.0. February 2021. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

HVA guidance can be found on the HVA PMO | CISA homepage.

- High Value Asset Control Overlay, Version 2.0, January 2021
- High Value Asset Control Overlay FAQ, Version 1.0, January 2018
- Securing High Value Assets, July 2018
- CISA Insights: Securing High Value Assets, September 2019
- Binding Operational Directive 18-02—Securing High Value Assets, May 2018

National Cybersecurity Protection System

NCPS guidance can be found on the NCPS Guidance Repository page.

- National Cybersecurity Protection System (NCPS) Cloud Interface Reference Architecture Volume 1: General Guidance, Version 1.4, May 2021
- National Cybersecurity Protection System (NCPS) Cloud Interface Reference Architecture Volume 2: Reporting Pattern Catalog DRAFT, Version 1.1, May 2021

Cybersecurity Shared Service Offering (formerly Quality Service Management Office)

- Quality Services Management Office Fact Sheet
- Centralized Mission Support Capabilities for the Federal Government (M-19-16), April 2019

Trusted Internet Connections

TIC guidance can be found on the TIC Guidance Repository page.

- Trusted Internet Connections 3.0 Program Guidebook, Version 1.1, July 2021
- Trusted Internet Connections 3.0 Reference Architecture, Version 1.1, July 2021
- Trusted Internet Connections 3.0 Security Capabilities Catalog, Version 2.0, October 2021
- Trusted Internet Connections 3.0 Traditional TIC Use Case, Version 1.0, April 2021
- Trusted Internet Connections 3.0 Branch Office Use Case, Version 1.0, April 2021
- Trusted Internet Connections 3.0 Remote User Use Case, Version 1.0, October 2021
- Trusted Internet Connections 3.0 Cloud Use Case, DRAFT, June 2022

Other CISA Resources

- Cloud Security Technical Reference Architecture
- Applying Zero Trust Principles to Enterprise Mobility
- Secure Cloud Business Applications (SCuBA) Technical Reference Architecture (TRA) (Draft)
- Extensible Visibility Reference Framework (eVRF) Guidebook (Draft)
- Multifactor Authentication
- Applying Zero Trust Principles to Enterprise Mobility
- Cyber Resilience Review Assessments
- govCAR Factsheet
- Cybersummit 2021 Session Day 2: Zero Trust