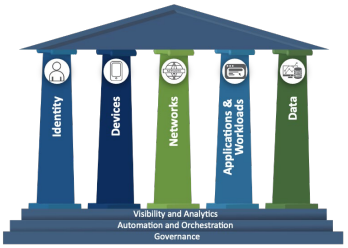
Zero Trust Maturity Model

Response to Comments

OVERVIEW



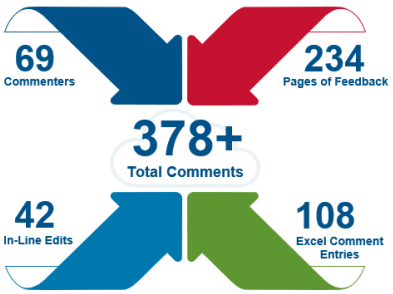
On 11 April 2023, the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) delivered an updated Zero Trust Maturity Model (ZTMM) draft—a roadmap for agencies to reference as they transition toward a zero trust architecture (ZTA).

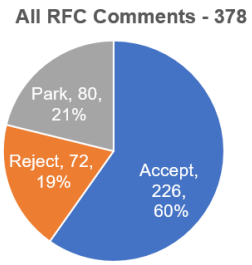
The published update is a result of many different inputs, including

- Comments gathered during the ZTMM V1.0 Request for Comment period from September to October 2021.
- A review of Zero Trust Implementation Plans with the Office of Management and Budget (OMB), as required by OMB's M-22-09.[1]
- Inputs from CyberStat Working Groups.
- Findings from National Security Telecommunications Advisory Committee (NSTAC) meetings.[2]
- Modernization deep dives.
- Individual one-on-one meetings with agencies, international partners, and the greater IT community.

REQUEST FOR COMMENT DETAILS

CISA issued a Request for Comment (RFC) period for the ZTMM from 7 September 2021 to 1 October 2021 and collected 378 comments from agencies, vendors, consulting services, academic organizations, trade associations, individuals, and foreign organizations.





CISA thanks all commenters and collaborators for their critical feedback and questions. CISA's analysis of the above inputs resulted in the ZTMM changes described in this document.

REVISED MATURITY EVOLUTION

Commenters requested additional guidance and space to evolve along the maturity model.

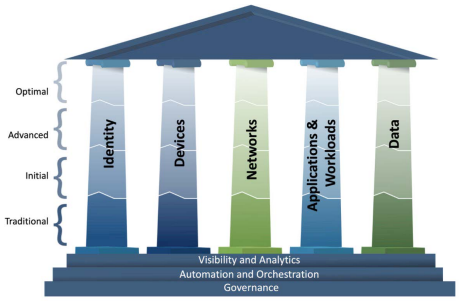
In response, CISA added the additional maturity stage "Initial" to the maturity model and realigned text for consistency across all pillars. CISA revised guiding criteria for each stage to account for the new maturity model stage. These maturity stages are meant to be dynamic; planned progress from stage to stage may shift in scope over time.

---

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

[2] "The President's NSTAC Meeting Resources," CISA, accessed March 8, 2023, https://www.cisa.gov/resources-tools/groups/presidents-national-security-telecommunications-advisory-committee/presidents-nstac-meeting-resources.

PURPOSE AND OMB ALIGNMENT



Commenters looked for updates to the longer-term ZTMM purpose.

In response to this, CISA updated the text preceding the model to reflect content updates and revised the purpose so the ZTMM is no longer a stopgap solution but continues to support agencies in designing and implementing their ZTA transition plans. The ZTMM has been aligned with OMB's M-22-09 "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles" (released January 2022) to include new and updated figures and highlight aspects of cybersecurity not included in the model.

EXPANDED CONTENT AND GUIDANCE

Commenters requested expanded content and guidance across all pillars and functions to provide more granularity to ZTA support implementation.

In response to this, CISA revised the text for every function of the model, expanded and added functions for each pillar, and clarified intent of cross-cutting pillars. Notable changes in specific stages include:

- **Identity:** Additional details provided in *Authentication* regarding "phishing-resistant MFA," including implementation of passwordless MFA via FIDO2 or PIV, addition of flexibility with *Identity Stores* that emphasizes integration across self-managed and hosted identity stores, and addition of a new *Access Management* function for tailored access.
- **Devices:** Updated *Policy Enforcement & Compliance* function to address software and configuration management; revised *Automation and Orchestration* and *Governance* to include deprovisioning, offboarding devices, and remediation steps for failure to meet posture requirements; and added *Device Threat Protections* function for centralized security management.
- **Networks:** Revised *Network Segmentation* function to promote microsegmentation based around application profiles and added *Network Traffic Management* function and *Network Resilience* function. Further revised pillar to incorporate elements of the original *Threat Protection* function into *Visibility & Analytics* and expanded *Traffic Encryption* function.
- **Applications and Workloads:** Updated *Application Access* function to incorporate contextual information, enforce expiration conditions, and adhere to least privilege principles. Revised *Application Threat Protections* and *Application Security Testing* to integrate protections into application workflows for real-time visibility and security testing throughout the software development life cycle. Incorporated a new *Secure Application Development and Deployment Workflow* function to formalize code deployment, restrict access to production environments, and promote a shift to immutable workloads. Renamed and revised *Application Accessibility* function to focus on making applications available to authorized users over public networks in alignment with OMB's M-22-09.
- **Data:** Expanded *Data Encryption* function to support encrypting data across the enterprise, formalize key management policies, and incorporate cryptographic agility; revised *Data Inventory Management* and added *Data Categorization* function to address maturity toward inventoried and understood data types; and added *Data Availability* function to optimize availability and emphasize access to historical data.
- **Cross-cutting Capabilities:** *Visibility and Analytics*, *Automation and Orchestration*, and *Governance* now include detailed scoping descriptions, pillar-independent paths to maturity, and updated recommendations across each pillar.

CLARIFIED TERMS AND CONCEPTS

Commenters shared feedback to clarify terms and concepts. In response, CISA included editorial edits, including adding and updating references, clarifying concepts throughout the ZTMM, and adding other general improvements to ensure consistency and improve flow.

For more information or to seek additional help, contact us at zerotrust@cisa.dhs.gov.