

Federal Trade Commission

OFFICE OF INSPECTOR GENERAL

August 30, 2023



Audit of FTC Progress on the Implementation of Zero Trust Architecture

FINAL REPORT • REDACTED • FOR PUBLIC RELEASE

Sensitive information on the FTC's information technology (IT) security systems, policies, and practices determined to be restricted from public release has been redacted from this document.

IN SUMMARY

Why We Performed This Audit

In August 2020, the National Institute of Standards and Technology (NIST) Information Technology Laboratory—the federal government’s technical leader for U.S. measurement and standards infrastructure—issued Special Publication (SP) 800-207, *Zero Trust Architecture*, to define and operationalize ZTA by providing “general deployment models and use cases where zero trust could improve an enterprise’s overall information technology security posture.”

Responding to an increasing number of high-profile security breaches (threatening the security of, among other entities, federal government networks), President Biden issued Executive Order (EO) 14028, *Improving the Nation’s Cybersecurity*. This order initiated government-wide efforts to ensure that security practices are in place, migrate the federal government to a ZTA, and realize the security benefits of cloud-based infrastructure while mitigating associated risks.

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issued its June 2021 *Zero Trust Maturity Model Pre-Decisional Draft* (Version 1.0) as a “stopgap solution” for federal government agencies creating ZTA implementation plans to comply with EO 14028.

OMB’s January 26, 2022, memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, required federal agencies to meet specific cybersecurity objectives and goals by the end of fiscal year (FY) 2024.

We conducted this audit to assess the Federal Trade Commission’s (FTC’s) progress on the implementation of ZTA and compliance with federal mandates.

Audit Results

The results of our research, interviews, FTC’s self-assessment, and inspection of relevant documentation inform our conclusions on the FTC’s implementation progress.

Based on our analysis of the FTC’s Office of the Chief Information Officer (OCIO) documentation provided to corroborate its self-assessment of the agency’s ZTA implementation status, we concluded that the FTC has made progress on meeting ZTA cybersecurity principles.

This audit report contains no recommendations for management.



Office of
Inspector
General

AUDIT
REPORT

*Audit of FTC
Progress
on the
Implementation
of Zero Trust
Architecture*

August 30, 2023

CONTENTS

Audit Results Summary..... 2
Why We Performed This Audit 3
Audit Results 7
Summary of Agency Response and OIG Comments 28
APPENDIX A: Objective, Scope, and Methodology 29
APPENDIX B: Summary of the Results of the FTC’S Self-Assessment 31
APPENDIX C: Acronyms and Abbreviations..... 34
APPENDIX D: FTC Management Response 35

AUDIT RESULTS SUMMARY

We conducted an audit to assess the Federal Trade Commission's (FTC's) progress on the implementation of zero trust architecture (ZTA) and compliance with federal mandates. We performed the audit work on FTC's ZTA implementation efforts from August 2022 through April 2023, measuring the agency's progress against standards set by the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency's (CISA's) *Zero Trust Maturity Model Pre-Decisional Draft*.

The results of our research, interviews, FTC's self-assessment,¹ and inspection of relevant documentation inform our conclusions on the FTC's implementation progress. Please see appendix A for additional information on our objective, scope, and methodology. Appendix B provides a complete summary of the results of the agency's self-assessment. Acronyms and abbreviations used in the report are listed in appendix C.

Based on our analysis of the FTC's Office of the Chief Information Officer (OCIO) documentation provided to corroborate its self-assessment of the agency's ZTA implementation status, we concluded that the FTC has made progress on meeting ZTA cybersecurity principles: to a greater extent, in the identity, device, and network pillars—and, to a lesser extent, in the application workload, and data pillars. For instance:

- The agency has implemented wide use of multifactor authentication (MFA), requiring a combination of a user's PIV badge as well as a unique code. At the time of our audit work, most of the FTC's IT systems require MFA.
- Further, the FTC has made progress with the ability to enforce least-privilege access, which requires each network user to be authorized and have a need to access certain areas of the network.

For further detail on the maturity status of the agency's ongoing ZTA implementation, please see Audit Results.

We have included no recommendations for management in this audit report.

¹ We requested that the FTC's Office of the Chief Information Officer (OCIO) provide us with a self-assessment of the agency's ZTA implementation progress against guidance included in CISA's *Zero Trust Maturity Model Pre-Decisional Draft*. FTC OCIO's self-assessment concluded on December 14, 2022.

WHY WE PERFORMED THIS AUDIT

National Institute of Standards and Technology (NIST) Special Publication (August 2020)

The NIST Information Technology Laboratory—the federal government’s technical leader for U.S. measurement and standards infrastructure—issued Special Publication (SP) 800-207, *Zero Trust Architecture*,² to define and operationalize ZTA by providing “general deployment models and use cases where zero trust could improve an enterprise’s overall information technology security posture.” Partially co-authored by CISA, NIST SP 800-207 established “zero trust” not as a singular, static concept but “an evolving set of cybersecurity paradigms” that shift IT security’s focus from the outer (“network-based perimeters”) in toward “users, assets, and resources.” Adopting this IT security posture, federal agencies assume “no implicit trust” in its assets or user based on location (either physical or network) or ownership (either enterprise or personal); authentication and authorization become functions that must be performed before a user can access a session with an enterprise resource. The publication concluded with a generalized roadmap for federal agencies to transition to a ZTA cybersecurity posture, from planning to deployment—prescribing an incremental implementation, rather than a “wholesale replacement of infrastructure or process,” that will introduce an “indefinite period” of hybrid ZTA-/perimeter-based IT security before an enterprise is fully modernized.

Executive Order (May 2021)

Responding to an increasing number of high-profile security breaches (threatening the security of, among other entities, federal government networks), President Biden issued Executive Order (EO) 14028, *Improving the Nation’s Cybersecurity*.³ This order initiated government-wide efforts to ensure that security practices are in place, migrate the federal government to a ZTA, and realize the security benefits of cloud-based infrastructure while mitigating associated risks.

EO 14028 directed heads of federal agencies to

- update existing agency plans to prioritize resources for the adoption and use of cloud technology as outlined in relevant Office of Management and Budget (OMB) guidance;
- develop a plan to implement zero trust architecture—including, as appropriate, (a) the migration steps outlined in NIST standards and

² [NIST, SP 800-207, ZERO TRUST ARCHITECTURE \(2020\)](#).

³ [EO 14028, 86 Fed. Reg. 26633 \(2021\)](#).

guidance,⁴ (b) any steps already completed, (c) activities that will have the most immediate security impact, and (d) a schedule to implement them; and

- provide a report to the Director of OMB and the Assistant to the President and National Security Advisor, describing the plans required for ZTA implementation and adoption.

Zero Trust Maturity Model (June 2021)

CISA issued its June 2021 *Zero Trust Maturity Model Pre-Decisional Draft* (Version 1.0) as a “stopgap solution” for federal government agencies creating ZTA implementation plans to comply with EO 14028. Even though CISA’s ZTA model would evolve—Version 2.0 was issued in April 2023—and the “rapidly evolving environment and technology landscape” maintains a perpetually uncertain future, the draft Version 1.0 clearly established the challenge that agencies face: at the core, legacy systems and enterprises that rely on an “implicit trust” that is proving maladaptive to current cybersecurity reality. A solution that CISA proposed in its draft Version 1.0 centered around a “maturity model” of incremental progress toward optimal zero-trust IT security. In this model, implementation of a ZTA is built upon a foundation of three IT security capabilities (visibility and analytics, automation and orchestration, and governance), on which rest five pillars of IT security components. These five components—along with the IT security functions that agencies must consider when designing and building their cybersecurity architecture—are defined in further detail in the Audit Results section of this report. As covered in the draft Version 1.0 maturity model, the five pillars are identified below:

⁴ [NIST SP 800-207](#).



To support the incremental implementation that NIST’s guidelines described, CISA’s pre-decisional draft Version 1.0 ZTA model details stages of maturity that agencies should expect to achieve. As agencies’ IT security postures mature, the functions and capabilities within (and across) the five pillars become more automated, integrated, and dynamic. This maturity model is detailed below:

Traditional	Manual configurations and assignment of attributes, static security policies, pillar-level solutions with coarse dependencies on external systems, least-function established at provisioning, proprietary and inflexible pillars of policy enforcement, manual incident response and mitigation deployment
Advanced	Some cross-pillar coordination, centralized visibility, centralized identity control, policy enforcement based on cross-pillar inputs and outputs, some incident response to pre-defined mitigations, increased detail in dependencies with external systems, some least-privilege changes based on posture assessments
Optimal	Fully automated assigning of attributes to assets and resources, dynamic policies based on automated/observed triggers, assets have self-enumerating dependencies for dynamic least-privilege access (within thresholds), alignment with open standards for cross-pillar interoperability, centralized visibility with historian functionality for point-in-time recollection of state

OMB Memorandum (January 2022)

OMB's January 26, 2022, memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, required federal agencies to meet specific cybersecurity objectives and goals by the end of fiscal year (FY) 2024. Envisioning a government-wide zero-trust approach to IT security—and reinforcing EO 14028—the OMB memorandum provided government agencies “highest-value starting points” (as opposed to “a comprehensive guide” that describes the result of “a fully mature zero trust architecture”), expressed using the pillars, functions, and capabilities established in CISA's *Zero Trust Maturity Model Pre-Decisional Draft*. OMB required agencies to develop implementation plans, as well as budget estimates, for their own ZTA.

AUDIT RESULTS

As part of our audit field work, we requested that the FTC’s OCIO complete a self-assessment on the Commission’s progress toward ZTA implementation.⁵ OCIO provided assertions on the current status of 31 distinct measurements of the 16 total functions, and 3 cross-cutting capabilities, that comprise the 5 pillars of the ZTA model.

The answer options available in the self-assessment were derived from a combination of the three maturity stages (**traditional**, **advanced**, and **optimal**) identified in the *Zero Trust Maturity Model Pre-Decisional Draft* and two additional options representing **progress made** between the three stages.

Traditional	Manual configurations and assignment of attributes, static security policies, pillar-level solutions with coarse dependencies on external systems, least-function established at provisioning, proprietary and inflexible pillars of policy enforcement, manual incident response and mitigation deployment
➡ ➡ (Traditional—with progress made toward Advanced)	
Advanced	Some cross-pillar coordination, centralized visibility, centralized identity control, policy enforcement based on cross-pillar inputs and outputs, some incident response to pre-defined mitigations, increased detail in dependencies with external systems, some least-privilege changes based on posture assessments
➡ ➡ (Advanced—with progress made toward Optimal)	
Optimal	Fully automated assigning of attributes to assets and resources, dynamic policies based on automated/observed triggers, assets have self-enumerating dependencies for dynamic least-privilege access (within thresholds), alignment with open standards for cross-pillar interoperability, centralized visibility with historian functionality for point-in-time recollection of state

⁵ The FTC’s self-assessment—based on guidance included in the Cybersecurity and Infrastructure Security Agency’s (CISA’s) June 2021 (Version 1.0) *Zero Trust Maturity Model Pre-Decisional Draft*—concluded on December 14, 2022, with updates on March 7, 2023. See appendix B for a complete summary of the results of the agency’s self-assessment. In April 2023, CISA issued Version 2.0 of its *Zero Trust Maturity Model*, which added a fourth maturity stage (**initial**) between traditional and advanced—as well as revisions made to some Version 1.0 functions, along with new functions added, under all five pillars.

Based on OCIO’s assertions, and our analysis of its supporting documentation, we concluded that the FTC has made progress toward the advanced maturity level across the 5 ZTA pillars—and appears capable of meeting most of the relevant OMB milestones for ZTA implementation by the end of FY 2024. Below, we detail the agency’s maturity status for each pillar, across all functions and capabilities—and highlight the significant work ahead for the FTC’s compliance with OMB’s deadline.⁶

Pillar 1: IDENTITY

CISA’s *Zero Trust Maturity Model Pre-Decisional Draft* refers to **identity** as one or more attributes “that uniquely describe an agency user or entity.” The model prescribes growing from the practice of relying on the user entering a password (presumably once) to validate identity, toward requiring “a combination of factors to validate and verify” identity continuously.

The authentication function is a critical component of the zero-trust security model’s identity pillar. Before they grant user/entity access to a resource, organizations should verify the identity with strong authentication, such as confirming identity using MFA. For example, organizations ask for something the user/entity knows (e.g., a password), has (e.g., a security token), or is (e.g., biometric data) before granting resource access.

Under this pillar, CISA delineates the features of a traditional, advanced, or optimal stage of maturity for each of three functions (**authentication**, **identity stores**, and **risk assessment**), as well as the three cross-cutting capabilities (**visibility and analytics**, **automation and orchestration**, and **governance**). Details of the FTC’s self-assessment of maturity level for each function/capability are provided below:

Pillar 1: IDENTITY			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Authentication	✓ → →		

To support the agency’s progress toward advanced maturity, OCIO documented how it *authenticates* government-owned government-operated (GOGO) users’ identity using MFA [REDACTED]

⁶ OMB M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, “requires agencies to achieve specific zero trust security goals” by the end of FY 2024. In our “Audit Results,” we summarize OMB’s strategic goals by pillar—as well as the FTC’s progress toward meeting them.

Pillar 1: IDENTITY			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Authentication	✓ → →		
Identity Stores	✓ → →		

At its traditional stage of maturity, the agency documented making progress toward an advanced use of *identity stores*

[REDACTED]

Pillar 1: IDENTITY			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Authentication	✓ → →		
Identity Stores	✓ → →		
Risk Assessment	✓		

The agency documented a traditional maturity for the *risk assessment* function

[REDACTED]

Pillar 1: IDENTITY			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Authentication	✓ → →		
Identity Stores	✓ → →		
Risk Assessment	✓		
Governance Capability	✓		

CISA⁷ gauges agencies’ *governance capability* according to how it defines and enforces “cybersecurity policies, procedures, and processes, within and across pillars, to manage an agency’s enterprise and mitigate security risks” that support ZTA principles and comply with federal requirements.

⁷ CISA, Cybersecurity Division. *Zero Trust Maturity Model*, Version 2.0 (April 2023), p. 11. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.



Currently at a traditional maturity level, the agency’s identity governance capability features [REDACTED].

Pillar 1: IDENTITY			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Authentication	✓ → →		
Identity Stores	✓ → →		
Risk Assessment	✓		
Governance Capability	✓		
Automation & Orchestration Capability	✓		

When referring to agencies’ ZTA *automation and orchestration capability*, CISA⁸ contemplates the “full use of automated tools and workflows that support security response functions across products and services, while maintaining oversight, security, and interaction” of their development.

Similar to its identity governance, OCIO documented [REDACTED]

⁸ Ibid.

Pillar 1: IDENTITY			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Authentication	✓ → →		
Identity Stores	✓ → →		
Risk Assessment	✓		
Governance Capability	✓		
Automation & Orchestration Capability	✓		
Visibility & Analytics Capability	✓ → →		

CISA⁹ defines agencies’ *visibility and analytics capability* in two parts: *visibility* as referring to “observable artifacts that result from the characteristics of and events within enterprise-wide environments,” and *analytics* referring to “cyber-related data [that] can help inform policy decisions, facilitate response activities, and build a risk profile” for developing proactive security measures.

The agency’s visibility and analytics capability is currently progressing toward advanced maturity. [REDACTED]

Below, we review OCIO’s projected timeline for bringing the FTC in compliance with OMB’s M-22-09 deadline for starting a ZTA:

Pillar 1: IDENTITY—OMB Government-Wide Requirements by the End of FY 2024: (and FTC Status)

1. Agencies must employ centralized identity management systems for agency users that can be integrated into applications and common platforms. (OCIO target date of completion: FY 2024, fourth quarter)
2. Agencies must use strong MFA throughout their enterprise. For agency staff, contractors, and partners, phishing-resistant MFA is required. (OCIO target date of completion: FY 2024, second quarter)

⁹ Ibid.

- When authorizing users to access resources, agencies must consider at least once device-level signal alongside identity information about the authenticated user. (OCIO target date of completion: FY 2024, fourth quarter)

Pillar 2: DEVICE

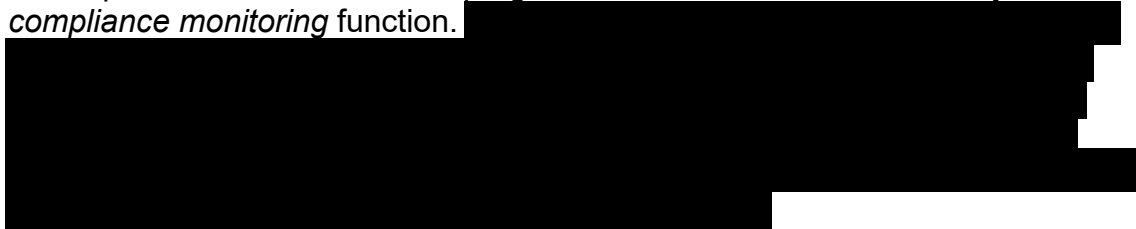
In its *Zero Trust Maturity Model Pre-Decisional Draft*, CISA defines a **device** as something tangible, “any hardware asset,” that can connect to an agency’s networks. Such assets can include “internet of things (IoT) devices, mobile phones, laptops, [and] servers.” CISA stresses the need to inventory and secure all of these assets, including “prevent unauthorized devices from accessing resources.”

This pillar highlights the challenges of controlling for a mixture of agency-owned and bring-your-own-device (BYOD) assets—future technology that might not be able to be anticipated and legacy devices—evaluating case-by-case entities and securing the risk of an agency-wide enterprise.

Under the devices pillar, CISA delineates the features of a traditional, advanced, or optimal stage of maturity for each of three functions (**compliance monitoring**, **data access**, and **asset management**), as well as the three cross-cutting capabilities (**visibility and analytics**, **automation and orchestration**, and **governance**). Details of the FTC’s self-assessment of maturity level for each function/capability are provided below:

Pillar 2: DEVICE			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Compliance Monitoring	✓ → →		

In this pillar, OCIO documented progress toward an advanced maturity for the *compliance monitoring* function.



AUDIT REPORT

Pillar 2: DEVICE			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Compliance Monitoring	✓ → →		
Data Access	✓ → →		

In its progress toward advanced maturity for the *data access* function, OCIO documented [REDACTED]

Pillar 2: DEVICE			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Compliance Monitoring	✓ → →		
Data Access	✓ → →		
Asset Management	✓ → →		


At traditional maturity for the *asset management* function, the agency has made some progress toward advanced. [REDACTED]

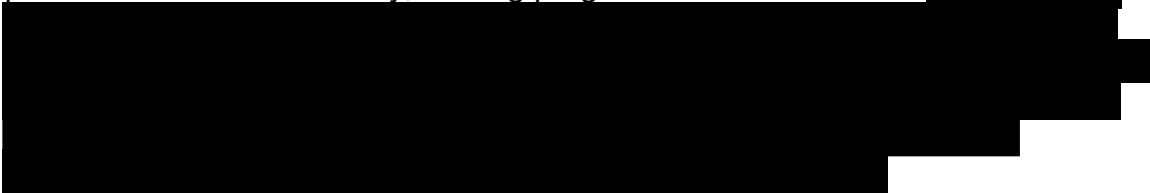
Pillar 2: DEVICE			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Compliance Monitoring	✓ → →		
Data Access	✓ → →		
Asset Management	✓ → →		
Governance Capability	✓ → →		

OCIO cited, as an example, the hardware specifications they established for an agency-wide laptop refresh to illustrate a *governance* capability at a traditional maturity (but making progress toward advanced). [REDACTED]



Pillar 2: DEVICE			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Compliance Monitoring	✓ → →		
Data Access	✓ → →		
Asset Management	✓ → →		
Governance Capability	✓ → →		
Automation & Orchestration Capability	✓ → →		

Similarly, OCIO self-assessed its *automation and orchestration* capability for this pillar at a traditional maturity, making progress toward advanced. 



Pillar 2: DEVICE			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Compliance Monitoring	✓ → →		
Data Access	✓ → →		
Asset Management	✓ → →		
Governance Capability	✓ → →		
Automation & Orchestration Capability	✓ → →		
Visibility & Analytics Capability	✓ → →		

OCIO also assessed the agency’s *visibility and analytics* capability at a traditional maturity level that is progressing toward advanced.

[REDACTED]

Pillar 2: DEVICE—OMB Government-Wide Requirements by the End of FY 2024: (and FTC Status)

1. Agencies must create reliable asset inventories through participation in CISA’s Continuous Diagnostics and Mitigation (CDM) program. (OCIO reported to OMB that it had coordinated exporting data from the FTC’s then-current vulnerability management program into the CDM program; [REDACTED])
2. Agencies must ensure their Endpoint Detection and Response (EDR) tools meet CISA’s technical requirements and are deployed widely. (OCIO reported to OMB that it anticipated needing to make minor modifications to the FTC’s EDR solution to meet technical requirements.)

Pillar 3: NETWORK/ENVIRONMENT

When CISA’s *Zero Trust Maturity Model Pre-Decisional Draft* advises agencies to re-examine their approaches to securing **networks**, it includes “open communications” media (e.g., intranet, wireless, and internet-based) channels. The new model stresses “segment[ing] and control[ing] networks” as it manages “internal and external data flows” for improved network defense.

ZTA represents a shift in IT security approach: from being “perimeter-focused,” with macro-segmentation and minimal restrictions, to an increasingly micro-segmented network posture, with increasingly constrained connectivity. Network segmentation separates a given network into subnetworks, facilitating security controls between the subnetworks, and decreasing the network’s attack surface. The FTC implements internal network segmentation using firewalls with features such as threat prevention and high throughput decryption.

Under this pillar, CISA delineates the features of a traditional, advanced, or optimal stage of maturity for each of three functions (**network segmentation**, **threat protection**, and **encryption**), as well as the three cross-cutting capabilities (**visibility and analytics**, **automation and orchestration**, and **governance**). Details of the FTC’s self-assessment of maturity level for each function/capability are provided below:

Pillar 3: NETWORK/ENVIRONMENT			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Network Segmentation	✓ → →		

The agency’s *network segmentation* is at traditional maturity, heading toward an advanced stage, according to OCIO’s self-assessment. [REDACTED]

Pillar 3: NETWORK/ENVIRONMENT			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Network Segmentation	✓ → →		
Threat Protection	✓		

OCIO assessed the agency’s current *threat protection* function at traditional maturity.

Pillar 3: NETWORK/ENVIRONMENT			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Network Segmentation	✓ → →		
Threat Protection	✓		
Encryption			✓

[REDACTED] It documented the agency's current configuration settings at an optimal maturity stage.

Pillar 3: NETWORK/ENVIRONMENT			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Network Segmentation	✓ → →		
Threat Protection	✓		
Encryption			✓
Governance Capability			✓

The agency's documentation of its network *governance* asserted a capability at an optimal maturity stage. [REDACTED]

Pillar 3: NETWORK/ENVIRONMENT			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Network Segmentation	✓ → →		
Threat Protection	✓		
Encryption			✓
Governance Capability			✓
Automation & Orchestration Capability	✓		

OCIO assessed the agency’s current *automation and orchestration capability* at the traditional maturity stage.

Pillar 3: NETWORK/ENVIRONMENT			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Network Segmentation	✓ → →		
Threat Protection	✓		
Encryption			✓
Governance Capability			✓
Automation & Orchestration Capability	✓		
Visibility & Analytics Capability	✓ → →		

Within this pillar, OCIO assessed the agency’s *visibility and analytics capability* at the traditional maturity stage, showing progress toward advanced maturity.



Pillar 3: NETWORKS—OMB Government-Wide Requirements by the End of FY 2024: (and FTC Status)

1. Agencies must resolve domain name system (DNS) queries using encrypted DNS wherever it is technically supported. (OCIO target date of completion: FY 2024, fourth quarter)
2. Agencies must enforce hypertext transfer protocol secure (HTTPS) for all web and application program interface (API) traffic in their environment. (OCIO target date of completion: FY 2024, fourth quarter)
3. (CISA will work with the Federal Risk and Authorization Management Program (FedRAMP) to evaluate government-wide solutions for encrypted email in transit and to make resulting recommendations to OMB.)
4. Agencies must develop a zero trust architecture plan that describes the agency’s approach to environmental isolation in consultation with CISA and submit to OMB as part of their zero trust implementation plan.



Pillar 4: APPLICATION WORKLOAD

Included in the CISA pre-decisional draft model’s consideration of agency’s **applications** and **workloads** are “systems, computer programs, and services” that users access and leverage “on-premise,” as well as “in a cloud environment.” The model calls for agencies to manage and secure the applications that they deliver to users.

Agencies should grant users access to specific resources based on their identity, context, and other relevant factors. As an agency’s ZTA posture matures, this pillar is supposed to ensure that its users have access only to the resources they need to perform their job functions (and nothing more), thereby reducing the risk of data breaches and unauthorized access. Accessibility matures through policies, combined with authentication and authorization mechanisms, to determine a user’s level of access to specific agency resources.

Under this pillar, CISA delineates the features of a traditional, advanced, or optimal stage of maturity for each of four functions (**access authorization**, **threat protections**, **accessibility**, and **application security**), as well as the three cross-cutting capabilities (**visibility and analytics**, **automation and orchestration**, and **governance**). Details of the FTC’s self-assessment of maturity level for each function/capability are provided below:



AUDIT REPORT

Pillar 4: APPLICATION WORKLOAD			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Access Authorization	✓		

OCIO documented its *access authorization* function at a traditional stage of maturity [REDACTED].

Pillar 4: APPLICATION WORKLOAD			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Access Authorization	✓		
Threat Protections	✓		

Similarly, OCIO assessed its *threat protections* function at a traditional stage of maturity. [REDACTED]

Pillar 4: APPLICATION WORKLOAD			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Access Authorization	✓		
Threat Protections	✓		
Accessibility		✓	

Regarding application workload *accessibility*, OCIO's agency self-assessment cited [REDACTED]. OCIO documented the agency's functional maturity at the advanced level.

Pillar 4: APPLICATION WORKLOAD			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Access Authorization	✓		
Threat Protections	✓		
Accessibility		✓	
Application Security	✓		

OCIO documented its *application security* function at a traditional stage of maturity [REDACTED].

Pillar 4: APPLICATION WORKLOAD			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Access Authorization	✓		
Threat Protections	✓		
Accessibility		✓	
Application Security	✓		
Governance Capability	✓		

Similarly, OCIO assessed its *governance capability* at a traditional stage of maturity [REDACTED].

Pillar 4: APPLICATION WORKLOAD			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Access Authorization	✓		
Threat Protections	✓		
Accessibility		✓	
Application Security	✓		
Governance Capability	✓		
Automation & Orchestration Capability	✓		

Likewise, OCIO assessed its *automation and orchestration capability* at a traditional stage of maturity [REDACTED].

Pillar 4: APPLICATION WORKLOAD			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Access Authorization	✓		
Threat Protections	✓		
Accessibility		✓	
Application Security	✓		
Governance Capability	✓		
Automation & Orchestration Capability	✓		
Visibility & Analytics Capability			✓

Regarding this pillar’s *visibility and analytics*, the agency documented a more mature capability [REDACTED]

[REDACTED] OCIO asserted that this capability is at an optimal stage of maturity.

Pillar 4: APPLICATIONS & WORKLOADS—OMB Government-Wide Requirements by the End of FY 2024: (and FTC Status)

1. Agencies must operate dedicated application security testing programs. (OCIO assertion: “FTC contract language will request that vendor provide manual expert analysis of their provided application.”)
2. Agencies must utilize high-quality firms specializing in application security for independent third-party evaluation. [REDACTED]
3. Agencies must maintain an effective and welcoming public vulnerability disclosure program for their internet-accessible systems. [REDACTED]

4. Agencies must identify at least one internal-facing Federal Information Security Management Act (FISMA) Moderate application and make it fully operational and accessible over the public internet. [REDACTED]
5. (CISA and the General Services Administration, or GSA, will work together to provide agencies with data about their online applications and other assets.)
6. Agencies should work toward employing immutable workloads when deploying services, especially in cloud-based infrastructure. [REDACTED]

Pillar 5: DATA

The *Zero Trust Maturity Model Pre-Decisional Draft* contemplates **data** residing “on devices, in applications, and [within] networks.” For this pillar, agencies are expected to account for (“inventory, categorize, and label”), as well as protect, all relevant assets—both what it stores and what it sends out or receives (i.e., data “at rest and in transit”).

Under the devices pillar, CISA delineates the features of a traditional, advanced, or optimal stage of maturity for each of three functions (***inventory management, access determination, and encryption***), as well as the three cross-cutting capabilities (***visibility and analytics, automation and orchestration, and governance***). Details of the FTC’s self-assessment of maturity level for each function/capability are provided below:

Pillar 5: DATA			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
<i>Inventory Management</i>	✓		

OCIO assessed its *inventory management* function at a traditional stage of maturity [REDACTED].

Pillar 5: DATA			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
<i>Inventory Management</i>	✓		
Access Determination	✓		

Similarly, OCIO assessed its *access determination* function at a traditional stage of maturity [REDACTED].

Pillar 5: DATA			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
<i>Inventory Management</i>	✓		
<i>Access Determination</i>	✓		
Encryption	✓ ➡ ➡		

The FTC submitted a self-assessment with the data *encryption* function at an initial maturity stage, with progress toward advanced. [REDACTED]

Pillar 5: DATA			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
<i>Inventory Management</i>	✓		
<i>Access Determination</i>	✓		
<i>Encryption</i>	✓ ➡ ➡		
Governance Capability	✓		

The agency assessed its *governance capability* at a traditional stage of maturity; [REDACTED]

Pillar 5: DATA			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Inventory Management	✓		
Access Determination	✓		
Encryption	✓ ➡ ➡		
Governance Capability	✓		
Automation & Orchestration Capability	✓ ➡ ➡		

The agency's self-assessment described an *automation and orchestration capability* at an initial maturity stage, with progress toward advanced.



Pillar 5: DATA			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Inventory Management	✓		
Access Determination	✓		
Encryption	✓ ➡ ➡		
Governance Capability	✓		
Automation & Orchestration Capability	✓ ➡ ➡		
Visibility & Analytics Capability	✓		

The agency assessed its *visibility and analytics capability* at a traditional stage of maturity.



Pillar 5: DATA—OMB Government-Wide Requirements by the End of FY 2024: (and FTC Status)

1. (Federal chief data officers and chief information security officers will create a joint committee to develop a zero trust data security guide for agencies.)
2. Agencies must implement initial automation of data categorization and security responses, focusing on tagging and managing access to sensitive documents. [REDACTED]
3. Agencies must audit access to any data encrypted at rest in commercial cloud infrastructure. [REDACTED]
4. Agencies must work with CISA to implement comprehensive logging and information-sharing capabilities, as described in OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*. [REDACTED]

SUMMARY OF AGENCY RESPONSE AND OIG COMMENTS

In its written response to this report, FTC OCIO management stated its intention of incorporating areas of improvement from the report into the agency's overall program plan. The FTC response to our report is included in its entirety in appendix D.

APPENDIX A: OBJECTIVE, SCOPE, AND METHODOLOGY

We conducted an audit to assess the FTC’s progress on the implementation of ZTA and compliance with federal mandates. As background for our audit, we researched and reviewed pertinent authorities, including federal laws, agency guidance, policies, and procedures. These included Executive Order 14028, *Improving the Nation’s Cybersecurity*¹⁰; OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*¹¹; OMB Circular A-123, *Management’s Responsibility for Enterprise Risk Management and Internal Controls*¹²; OMB Circular A-130, *Managing Information as a Strategic Resource*¹³; the U.S. Government Accountability Office (GAO) *Standards for Internal Control in the Federal Government*¹⁴; internal FTC policies; and policy memoranda.

As part planning for the audit, we reviewed relevant oversight products and developed an understanding of internal controls that are material to the audit objective. We compared the Commission’s plan for ZTA implementation against CISA’s recommended approach to ZTA, which incorporated in CISA’s *Zero Trust Maturity Model Pre-Decisional Draft*. To gain further insight, we conducted interviews with key FTC officials on the plans for ZTA implementation.

Finally, we requested that FTC OCIO complete a self-assessment on the Commission’s ZTA progress. To corroborate the results that OCIO included in its self-assessment, we reviewed policies and other documents (e.g., screenshots, device inventory listings, and scan results provided by OCIO) supporting the assertions made by OCIO officials. We used the results of our research, interviews, the FTC’s self-assessment, and documentation review to conclude on the status of the FTC’s implementation of ZTA.

We performed the audit work remotely from August 2022 through April 2023. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

¹⁰ [EO 14028, 86 Fed. Reg. 26633 \(2021\)](#)

¹¹ OMB, OMB Memo No. M-22-09, MOVING THE U.S. GOVERNMENT TOWARD ZERO TRUST CYBERSECURITY PRINCIPLES (2022).

¹² OMB, OMB Circular A-123, MANAGEMENT’S RESPONSIBILITY FOR ENTERPRISE RISK MANAGEMENT AND INTERNAL CONTROL (2016).

¹³ OMB, OMB Circular A-130, MANAGING INFORMATION AS A STRATEGIC RESOURCE (2016).

¹⁴ GAO, GAO-14-704G, ACCOUNTABILITY OFFICE (GAO) STANDARDS FOR INTERNAL CONTROL IN THE FEDERAL GOVERNMENT (2014).

We used the following criteria in the performance of our review:

- Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021)
- GAO, *Standards for Internal Control in the Federal Government*
- OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (January 26, 2022)
- OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*
- OMB A-130, *Managing Information as a Strategic Resource*
- NIST SP 800-207, *Zero Trust Architecture*

APPENDIX B: SUMMARY OF THE RESULTS OF THE FTC’S SELF-ASSESSMENT

Pillar 1: IDENTITY			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
<i>Authentication</i>	✓ ➡ ➡		
<i>Identity Stores</i>	✓ ➡ ➡		
<i>Risk Assessment</i>	✓		
<i>Governance Capability</i>	✓		
<i>Automation & Orchestration Capability</i>	✓		
<i>Visibility & Analytics Capability</i>	✓ ➡ ➡		
Pillar 2: DEVICE			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
<i>Compliance Monitoring</i>	✓ ➡ ➡		
<i>Data Access</i>	✓ ➡ ➡		
<i>Asset Management</i>	✓ ➡ ➡		
<i>Governance Capability</i>	✓ ➡ ➡		
<i>Automation & Orchestration Capability</i>	✓ ➡ ➡		
<i>Visibility & Analytics Capability</i>	✓ ➡ ➡		

Pillar 3: NETWORK/ENVIRONMENT			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Network Segmentation	✓ → →		
Threat Protection	✓		
Encryption			✓
Governance Capability			✓
Automation & Orchestration Capability	✓		
Visibility & Analytics Capability	✓ → →		
Pillar 4: APPLICATION WORKLOAD			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
Access Authorization	✓		
Threat Protections	✓		
Accessibility		✓	
Application Security	✓		
Governance Capability	✓		
Automation & Orchestration Capability	✓		
Visibility & Analytics Capability			✓

AUDIT REPORT

Pillar 5: DATA			
FUNCTION/ CAPABILITY	Traditional MATURITY	Advanced MATURITY	Optimal MATURITY
<i>Inventory Management</i>	✓		
<i>Access Determination</i>	✓		
<i>Encryption</i>	✓ → →		
<i>Governance Capability</i>	✓		
<i>Automation & Orchestration Capability</i>	✓ → →		
<i>Visibility & Analytics Capability</i>	✓		

APPENDIX C: ACRONYMS AND ABBREVIATIONS

AD	active directory
BYOD	bring-your-own-device
CDM	Continuous Diagnostics and Mitigation
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
EDR	Endpoint Detection and Response
EO	Executive Order
FISMA	Federal Information Security Management Act
FTC	Federal Trade Commission
FY	fiscal year
GAO	U.S. Government Accountability Office
GFE	government-furnished equipment
GOGO	government-owned government-operated
GSS	general support system
HCMO	Human Capital Management Office
IoT	internet of things
MFA	multifactor authentication
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
TIC	Trusted Internet Connection
ZTA	zero trust architecture

APPENDIX D: FTC MANAGEMENT RESPONSE



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580
MEMORANDUM

DATE: August 7, 2023
FROM: Mark Gray, Chief Information and Chief Data Officer
TO: Andrew Katsaros, Inspector General
SUBJECT: Management's Response to the Audit of Federal Trade Commission (FTC)
Progress on the Implementation of Zero Trust Architecture (ZTA)

FTC Management appreciates the report produced by the Office of the Inspector General (OIG). The agency will use the analysis to improve and strengthen its Information Security Program.

The report recognizes the FTC has made progress toward the ZTA advanced maturity level across the five ZTA pillars, as indicated by ratings of "Traditional—with progress made toward Advanced" for three of the five Zero Trust Pillars and "Traditional" for Application Workload and Data pillars. The agency will incorporate areas of improvement from the report, into the agency's overall program plan.

The FTC is committed to continually improving its Information Security through continued partnership with the OIG.

A handwritten signature in black ink, appearing to read "Mark Gray".

Digitally signed by MARK GRAY
Date: 2023.08.07 14:29:27 -04'00'

Mark Gray, Chief Information Officer and Chief Data Officer