U.S. Consumer Product Safety Commission
OFFICE OF INSPECTOR GENERAL

Audit of the CPSC's Zero Trust Implementation

May 5, 2026

26-A-02

VISION STATEMENT

We are agents of positive change striving for continuous improvements in our agency's management and program operations, as well as within the Office of Inspector General.

STATEMENT OF PRINCIPLES

We will:

Work with the Commission and the Congress to improve program management.

Maximize the positive impact and ensure the independence and objectivity of our audits, investigations, and other reviews.

Use our investigations and other reviews to increase government integrity and recommend improved systems to prevent fraud, waste, and abuse.

Be innovative, question existing procedures, and suggest improvements.

Build relationships with program managers based on a shared commitment to improving program operations and effectiveness.

Strive to continually improve the quality and usefulness of our products.

Work together to address government-wide issues.

May 5, 2026

TO: Peter A. Feldman, Acting Chairman

FROM: Christopher W. Dentel, Inspector General CHRISTOPHER DENTEL Digitally signed by CHRISTOPHER DENTEL Date: 2026.05.05 10:30:33 -04'00'

SUBJECT: Audit of the CPSC's Adoption of Zero Trust Requirements

Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, requires federal agencies to strengthen their cybersecurity posture. This EO mandates the adoption of cyber security best practices and accelerates the transition to a Zero Trust (ZT) architecture (ZTA). ZT is a security approach that assumes no user, device, or system can be trusted by default. Access to organizational information is not granted based on where someone is connected from or who owns the device; rather, every access request is verified before access is authorized. To assess agency adoption of ZT requirements, the Consumer Product Safety Commission (CPSC) Office of Inspector General (OIG) retained Williams, Adley & Co.-DC LLP (Williams Adley), an independent public accounting firm, to perform an audit of the CPSC's ZT implementation.

Under a contract monitored by the OIG, Williams Adley issued a report to document the results of its audit. The contract required that the audit be performed in accordance Government Auditing Standards, issued by the Comptroller General of the United States. We reviewed the resulting report and related documentation. We made relevant inquiries to the contractors. Our review was not intended to enable us to express, and we do not express, an opinion on the matters contained in the report. Williams Adley is responsible for the attached report. However, our review disclosed no instances where Williams Adley did not comply, in all material respects, with Government Auditing Standards. Overall, the audit confirmed that the CPSC had begun implementing the technical controls that establish a foundation for a true ZTA. The CPSC concurred with William Adley's conclusions and indicated it plans to continue to invest in additional ZT solutions which would enable the full adoption of a ZTA where no user, device, or system will be trusted by default.

Williams Adley did not issue any Notices of Findings, indicating that the CPSC's current ZT trajectory is aligned with federal cybersecurity modernization objectives and supports the continued development of a more secure and resilient information security environment. However, Williams Adley provided two suggestions to support the CPSC's continued progress toward achieving an "Advanced" level of ZT implementation maturity.

Should you have any questions about this report, please contact me at cdentel@cpsc.gov.

Table of Contents

ABBREVIATIONS AND SHORT TITLES

CISA	**Cybersecurity and Infrastructure Security Agency**
CDM	**Continuous Diagnostics and Mitigation**
CPSC	**U.S. Consumer Product Safety Commission**
EO	**Executive Order**
EXIT	**Office of Information and Technology Services**
IoT	**Internet of Things**
M	**Memorandum**
MFA	**Multi-factor Authentication**
NIST	**National Institute of Standards and Technology**
OMB	**Office of Management and Budget**
SOAR	**Security Orchestration, Automation, and Response**
SP	**Special Publication**
Williams Adley	**Williams, Adley, & Co.-DC LLP**
ZTMM	**Zero Trust Maturity Model**
ZT	**Zero Trust**
ZTA	**Zero Trust Architecture**

EXECUTIVE SUMMARY

Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, established a transformative policy direction for federal agencies to strengthen their cybersecurity posture. This EO mandates the adoption of security best practices and accelerates the transition to a Zero Trust (ZT) architecture (ZTA). ZT is a security approach that assumes no user, device, or system can be trusted by default. Access to organizational information is not granted based on where someone is connected from or who owns the device; rather, every access request is verified before access is authorized.

In order to determine if the Consumer Product Safety Commission (CPSC) has achieved the adoption of ZT requirements, the CPSC Office of Inspector General contracted with Williams, Adley & Co.-DC LLP (Williams Adley) to perform an audit of the CPSC's ZT implementation. The primary objective of this audit was to assess the CPSC's implementation of its ZT strategy in accordance with the Office of Management and Budget (OMB) Memorandum (M)-22-09 and the Cybersecurity and Infrastructure Security Agency (CISA)'s Zero Trust Maturity Model (ZTMM) Version 2.0.

CISA's ZTMM is structured around five (5) core pillars: Identity, Devices, Networks, Applications and Workloads, and Data. These five pillars are further supported by three (3) cross-cutting capabilities that enhance ZT implementation: Visibility and Analytics, Automation and Orchestration, and Governance. The ZTMM outlines four (4) progressive maturity levels that reflect an organization's advancement in adopting ZT principles: Traditional, Initial, Advanced, and Optimal. The Objectives and Scope section of this report provides additional context regarding the parameters of the audit.

Overall, the audit confirmed that the CPSC is currently operating at the "Traditional" and "Initial" maturity levels of ZT implementation as defined in the ZTMM. Specifically, Williams Adley verified the presence of baseline ZT controls across all five ZTMM pillars and supporting cross-cutting capabilities. The CPSC provided a ZT self-assessment and met the requirements as established in OMB M-22-09 to provide a ZT strategy. Williams Adley's assessment of the maturity of the CPSC's ZT implementation matched the CPSC's self-assessment. The CPSC has begun implementing the technical controls that establishes a foundation for a true ZTA. The CPSC has indicated it plans to continue to invest in additional ZT solutions which would enable the full adoption of a ZTA where no user, device, or system will be trusted by default.

Williams Adley did not issue any Notices of Findings, indicating that the CPSC's current ZT trajectory is aligned with federal cybersecurity modernization objectives and supports the continued development of a more secure and resilient information security environment. However, Williams Adley provided two (2) suggestions to support CPSC's continued progress toward achieving an "Advanced" level of ZT implementation maturity. On April 28, 2026, Williams Adley obtained management's comments from the agency on the audit results presented in this report.

1. OBJECTIVE

The objective of this audit was for Williams, Adley & Co-DC LLP (Williams Adley) to perform an assessment of the Consumer Product Safety Commission's (CPSC) implementation of Zero Trust (ZT) requirements and its associated pillars in accordance with Office of Management and Budget (OMB) memorandum (M)-22-09, National Institute of Standards and Technology (NIST) Special Publications (SPs), and Zero Trust Maturity Model (ZTMM) Version 2.0 and associated internal controls.

2. ZERO TRUST OVERVIEW

In recent years, the federal government has recognized the urgent need to modernize its cybersecurity posture in response to increasingly sophisticated and persistent cyber threats. Traditional security models, which rely heavily on perimeter defenses and implicit trust within networks, have proven inadequate in protecting sensitive data and systems. To address these vulnerabilities, the government is transitioning to a ZT architecture (ZTA), a strategic approach to cybersecurity that assumes no user, device, or system should be trusted by default, regardless of whether it is inside or outside the network perimeter.

ZTA is an enterprise-wide cybersecurity framework that applies ZT principles to guide the design of component relationships, workflow planning, and access control policies. A ZT Enterprise refers to the resulting network infrastructure both physical and virtual—and the operational policies established through the implementation of a ZT strategy.

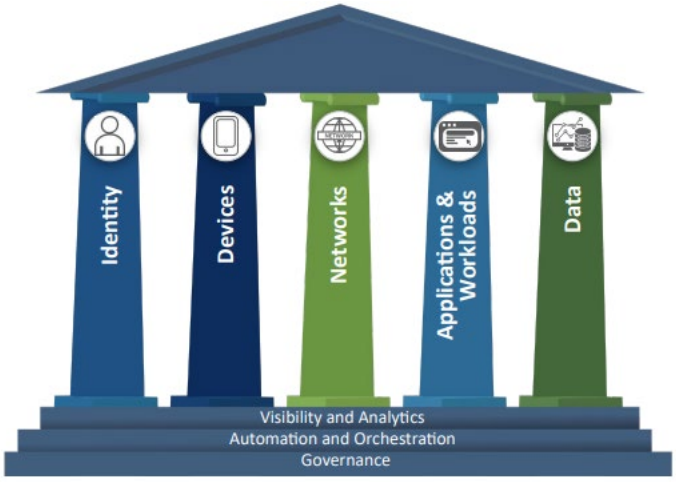
In August 2020, the NIST issued SP 800-207 to provide guidance to federal agencies on how to migrate and deploy ZT security concepts to an enterprise environment. The guidance states that a ZT approach is primarily focused on data and service protection but can and should be expanded to include all enterprise assets (devices, infrastructure components, applications, virtual and cloud components) and subjects (end users, applications and other nonhuman entities that request information from resources).

In May 2021, Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, established federal policy directing agencies to adopt security best practices, advance toward ZTA, and enhance the security of cloud services by implementing protective controls and mitigation measures. The EO also emphasized centralizing and streamlining access to cybersecurity data to enable effective analytics for identifying, assessing, and managing cybersecurity risks, and investing in both technology and personnel to support these modernization objectives. To support these efforts, agencies were required to perform the following actions within 60 days:

- Update existing agency plans to prioritize resources for the adoption and use of cloud technology.
- Develop a plan to implement ZT.
- Provide a report to the Director of OMB and the Assistant to the President and National Security Advisor discussing the plans.

In January 2022, OMB issued M-22-09, *Moving the U.S. Government Towards Zero Trust Cybersecurity Principles,*[1] establishing a ZT strategy aligned to CISA's ZTMM[2] and requiring agencies to meet specific cybersecurity standards and objectives by the end of fiscal year 2024, which emphasized enhanced identity verification, Multifactor Authentication (MFA), encryption and continuous monitoring to secure networks, systems, and data to minimize risk from both internal and external threats. M-22-09 served as a starting point for agencies transitioning from a conventional, perimeter-based defense to a ZT approach. ***Figure 1*** (below) showcases the five pillars of ZTMM – 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. The ZTMM provides a framework to achieve continuous modernization efforts related to ZT within a rapidly evolving environment and technology landscape.

Figure 1 **– Five Pillars of ZTMM**



Source: Cybersecurity and Infrastructure Security Agency[3]

Pillar 1: Identity

An identity refers to an attribute or set of attributes that uniquely describes an agency user or entity, including non-person entities. M-22-09 envisions that agency staff use enterprise-managed identities to access the applications they use in their work. Phishing-resistant MFA protects those personnel from sophisticated online attacks. The Identity pillar of the ZTMM ensures that every user is continuously verified and granted access. It relies on strong, phishing-resistant authentication, centralized identity systems, and least-privilege access controls. Continuous monitoring, automation, and governance work together to detect suspicious behavior, respond quickly to threats, and manage identities securely.

[1] Office of Management and Budget, "M-22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles".
[2] Cybersecurity and Infrastructure Security Agency, Zero Trust Maturity Model Version 2.0.
[3] Ibid., 7.

Pillar 2: Devices

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

M-22-09 envisions that agencies maintain a complete inventory of every device authorized and operated for official business and can prevent, detect, and respond to incidents on those devices. The Devices pillar in the ZTMM ensures that only trusted, secure, and compliant devices can access enterprise resources. It continuously evaluates device posture, lifecycle, and risk, while detecting and responding to threats in real time. Automation, visibility, and governance work together to enforce security policies, reduce risk from compromised or unmanaged devices, and maintain oversight.

Pillar 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.

M-22-09 envisions that agencies encrypt all Domain Name System requests and Hypertext Transfer Protocol traffic within their environment and begin executing a plan to break down their perimeters into isolated environments. The Network pillar of the ZTMM ensures that network access is tightly controlled, continuously monitored, and never implicitly trusted. It limits attacker movement through segmentation, encrypts all traffic, and grants access based on identity, device posture, and risk. Automation, visibility, and governance enable the network to rapidly detect threats, enforce policy consistently, and remain resilient against disruptions and attacks.

Pillar 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.

M-22-09 envisions that agencies treat all applications as internet-connected, routinely subject their applications to rigorous empirical testing, and welcome external vulnerability reports. The Applications & Workloads pillar of the ZTMM ensures that applications are securely developed, deployed, and accessed based on continuous risk evaluation. It enforces least-privilege access, protects applications from runtime threats, and embeds security throughout the development lifecycle. Visibility, automation, and governance work together to detect misuse, reduce vulnerabilities, and protect workloads across environments.

Pillar 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.

M-22-09 envisions that agencies are on a clear, shared path to deploy protections that make use of thorough data categorization. Furthermore, agencies take advantage of cloud security services and tools to discover, classify, and protect their sensitive data, and have implemented enterprise-wide logging and information sharing. The Data pillar of the ZTMM ensures that data is identified, protected, and accessed based on sensitivity and risk, regardless of where it resides. It applies strong access controls and encryption while continuously monitoring how data is used and moved. Automation and governance help maintain data availability, prevent unauthorized access or loss, and ensure compliance.

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:

1. Visibility and Analytics Capability – Provides real-time telemetry, monitoring, and analytics across all pillars to detect anomalies, assess risk, and support decision-making.
2. Automation and Orchestration Capability – Enables automated enforcement of policies, incident response, and integration across security tools to reduce manual effort and improve consistency.
3. Governance Capability – Establishes enterprise-wide policies, roles, responsibilities, and oversight mechanisms to ensure accountability and alignment with strategic goals.

As stated within the ZTMM, agencies should use the following guiding criteria to identify maturity for each ZT pillar/function and provide consistency across the maturity model. The maturity model is divided into four (4) levels with increasing levels of automation, as described below in ***Figure 2:***[4]

[4] Zero Trust Maturity Model Version 2.0.

Figure 2 – Zero Trust Maturity Levels and Descriptions

Maturity Level	Description
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 (1) 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.

Source: Cybersecurity and Infrastructure Security Agency

3. AUDIT RESULTS

3.1 The CPSC Zero Trust Assessment

This section presents an overview of the CPSC's ZT implementation status and the maturity levels achieved across the five ZT pillars and supporting cross-cutting capabilities, in accordance with the CISA's ZTMM and the federal ZTA strategy outlined in OMB M-22-09. Williams Adley's audit was designed to assess the CPSC's progress toward the federal government's mandated transition to ZTA and to establish a baseline understanding of the CPSC's current ZT capabilities relative to CISA-defined maturity levels.

Each function within the respective ZT pillars and cross-cutting capabilities was assessed independently, with results mapped to the corresponding ZTMM maturity levels (Traditional, Initial, Advanced, and Optimal). This structured approach aligns with CISA's guidance for assessing discrete ZT capabilities while supporting an enterprise-wide view of progress toward a fully integrated ZTA. The audit was performed against the CPSC's existing ZT self-assessment to validate that the assessed maturity levels accurately reflect the current operating environment and that implemented ZT controls are operating as described, consistent with the continuous verification principles emphasized in OMB M-22-09.

Within the CPSC, the Office of Information Technology Services (EXIT), led by the Chief Information Officer, is responsible for implementing and overseeing the agency's information security program, including CPSC's ZT strategy and execution. Consistent with ZT implementation guidance, achieving an effective ZTA requires enterprise-wide adoption of ZT principles and cannot be accomplished by EXIT alone. Rather, successful implementation depends on coordinated governance, shared accountability, and sustained collaboration among EXIT and other offices within the CPSC, including system owners, mission and business units, and organizations responsible for identity, data, and risk management.

Accordingly, EXIT coordinated with multiple offices within the CPSC and collaborated with a third-party contractor in 2024 to measure the agency's progress in implementing ZT requirements through a formal self-assessment aligned to the ZTMM. This collaborative assessment effort reflects CISA's emphasis on enterprise participation and cross-functional engagement as foundational elements of ZT adoption. The results of CPSC's self-assessment are presented in the sections below. Specifically, the maturity level assessed for each pillar function and cross-cutting capability from the February 2024 self-assessment is documented and compared to the maturity level independently assessed by Williams Adley.

Overall, as detailed in the sections below, Williams Adley determined that the CPSC is currently operating at the "Traditional" and "Initial" maturity levels of ZT implementation as defined by the ZTMM. At these maturity levels, agencies have established legacy and foundational controls that begin to support ZT outcomes but have not yet enabled dynamic, risk-based access decisions across the enterprise. Williams Adley verified the presence of baseline ZT-aligned technical and procedural controls across all five ZTMM pillars and supporting cross-cutting capabilities. Williams

Adley's independent assessment aligned with the results of the CPSC's self-assessment, indicating that the CPSC has developed an accurate understanding of its current ZT posture. The CPSC has achieved the foundational capabilities that are consistent with the early stages of ZT adoption described in the ZTMM and has established the groundwork for more advanced capabilities such as continuous authentication, least-privilege access enforcement, and real-time risk evaluation. As of March 2026, discussions with EXIT personnel indicated that the CPSC plans to continue investing in additional ZT solutions, governance processes, and technical integrations to progress toward "Advanced" maturity levels as defined by the ZTMM and in alignment with OMB M-22-09 objectives. Implementation of a mature ZTA will require EXIT to continue strengthening coordination with other offices across the CPSC to ensure ZT principles are consistently integrated into system development, operational processes, and enterprise risk management activities. Continued enterprise-wide collaboration will be critical to achieving the federal ZT vision articulated by OMB and CISA, in which no user, device, application, or system is trusted by default and access decisions are continuously evaluated based on risk, context, and policy.

3.1.1 Pillar 1: Identity & Cross-Cutting Capabilities

The Identity pillar ensures that access decisions are based on verified, context-aware identities rather than static credentials. This includes strong identity governance, phishing-resistant MFA, dynamic access controls, and automated identity orchestration. These capabilities help ensure that only the right individuals, using trusted devices, can access the right resources at the right time. *Table 1* below represents the CPSC's and Williams Adley's assessment of the maturity level for each function under the Identity pillar.

Table 1 – Maturity Levels for the Identity Pillar Functions

Function	CPSC's Self-Assessment	Williams Adley's Assessment
Authentication	Initial	Initial
Identity Stores	Initial	Initial
Risk Assessments	Traditional	Traditional
Access Management	Initial	Initial
Visibility and Analytics Capability[5]	Initial	Initial
Automation and Orchestration Capability	Traditional	Traditional
Governance Capability	Traditional	Traditional

Source: Williams Adley's summary of CPSC and Williams Adley information

[5] Functions denoted as a "Capability" are associated with the "cross-cutting" capabilities that impact multiple ZT pillars.

Results
Williams Adley determined the Identity pillar to be operating at the "Traditional" and "Initial" maturity levels. The following summarizes activities completed by the CPSC related to each Identify pillar function and cross-cutting capability:

- Authentication: The CPSC employs phishing resistant-MFA and incorporates contextual entity validation, including device posture, location, and user activity, to enforce access controls.
- Identity Stores: The CPSC operates a combination of self-managed identity repositories and hosted identity stores (e.g., cloud stores) with integration and capabilities such as Single Sign-On.
- Risk Assessments: The CPSC performs identity risk determinations, with evaluation of the likelihood that an identity has been compromised.
- Access Management: The CPSC authorizes access, including privileged access, through timebound controls with automated review and expiration. The CPSC has implemented the use of identity security solutions and regular privileged access reviews, ensuring continuous validation of elevated access.
- Visibility and Analytics Capability: The CPSC has implemented capabilities to collect and retain detailed user and entity activity logs and performs routine analysis through a combination of manual review and automated methods. The CPSC collects log data to support review which includes key contextual attributes, such as time generated, operation name, result status, identity performing the action, and target resources affected. In addition, the CPSC uses industry-standard tools to support identification for the cloud-based public-facing systems requiring authentication.
- Automation and Orchestration Capability: The CPSC manually orchestrates identity onboarding, offboarding, and disabling processes for self-managed identities, with integration across systems. The CPSC conducts access reviews to confirm that access privileges remain current, authorized, and aligned with least-privilege principles. As part of this review process, any discrepancies that are identified will be coordinated with the appropriate office to ensure timely deactivation of the accounts which no longer require access.
- Governance Capability: The CPSC has established Identity, Credential, and Access Management and related policies with clearly defined scopes, as well as documented roles and responsibilities to support governance.

3.1.2 Pillar 2: Devices & Cross-Cutting Capabilities

The Devices pillar ensures that only authorized and secure devices are permitted to access agency resources. This includes continuous monitoring of device health, compliance with security configurations, and automated enforcement of access policies based on device posture. These controls help reduce the risk of unauthorized access and ensure that endpoints meet security standards before connecting to sensitive systems. ***Table 2*** below represents the CPSC's and Williams Adley's assessment of the maturity level for each function under the Devices pillar.

Table 2 – Maturity Levels for the Devices Pillar Functions

Function	CPSC's Self-Assessment	Williams Adley's Assessment
Policy Enforcement & Compliance Monitoring	Initial	Initial
Asset & Supply Chain Risk Management	Traditional	Traditional
Resource Access	Traditional	Traditional
Device Threat Protection	Initial	Initial
Visibility and Analytics Capability	Initial	Initial
Automation and Orchestration Capability	Initial	Initial
Governance Capability	Traditional	Traditional

Source: Williams Adley's summary of CPSC and Williams Adley information

Results

Williams Adley determined the Devices pillar to be operating at the "Traditional" and "Initial" maturity levels. The following summarizes activities completed by the CPSC related to each Devices pillar function and cross-cutting capability:

- Policy Enforcement & Compliance Monitoring: The CPSC collects self-reported device attributes, including credentials, cryptographic keys, tokens, and user associated data, to inform device awareness. The CPSC has established processes to support device governance. Specifically, an approval process exists for authorized software usage, and the CPSC can deploy software updates, configuration changes, and patches to managed devices.
- Asset & Supply Chain Risk Management: The CPSC has deployed tools to monitor third-party risks and reviews supplier risk profiles, including during the assessment and authorizations process. Besides these periodic assessments, the CPSC also monitors risk events such as bankruptcies, cyber incidents, and other supply chain disruptions related to third-parties.
- Resource Access: The CPSC leverages an enterprise network access control and identity management tool that includes device profiling policy capabilities. The profiling interface presents an extensive set of default policies designed to identify and classify endpoint device types, including mobile endpoints, printers, IoT devices, and network infrastructure components such as access points.
- Device Threat Protection: The CPSC has implemented automated processes to deploy and update threat protection capabilities across managed endpoints and virtual assets. These processes are supported by integrated policy enforcement and compliance monitoring functions, enabling the CPSC to maintain baseline security controls and monitor adherence to defined security requirements across the devices.

- Visibility and Analytics Capability: The CPSC has deployed asset management capabilities through the Continuous Diagnostics and Mitigation (CDM) program. The CPSC leverages CDM's passive and active scanning capabilities to identify, track, and manage hardware and software assets across its network. Asset information is routinely monitored via the CDM Dashboard, which provides visibility into hardware and software assets within the CPSC's environment.
- Automation and Orchestration Capability: The CPSC leverages automation through tools and scripted workflows to support device and virtual asset lifecycle management. These capabilities are used to automate provisioning, configuration, registration, and deprovisioning activities, improving consistency and reducing manual processes. In addition, centrally managed endpoint security and device management platforms are deployed across the CPSC's IT environment and are actively monitoring device compliance, including patch levels and network access controls. These capabilities are also used to deploy configuration changes and software updates with the objective of supporting ongoing device hygiene and incremental progress toward a more mature ZT device posture.
- Governance Capability: The CPSC has developed configuration management policies and procedures for IT hardware and software inventories, as well as server patching, and has drafted supporting supply chain risk management procedures. The CPSC has also implemented a software approval and control process for CPSC-managed devices which is demonstrated by documented software approval workflows and application whitelisting practices.

3.1.3 Pillar 3: Networks & Cross-Cutting Capabilities

The Networks pillar ensures that security controls are applied throughout an agency's infrastructure to enhance traditional protections and strengthen data defense. *Table 3* below represents the CPSC's and Williams Adley's assessment of the maturity level for each function under the Networks pillar.

Table 3 – Maturity Levels for the Networks Pillar Functions

Function	CPSC's Self-Assessment	Williams Adley's Assessment
Network Segmentation	Traditional	Traditional
Network Traffic Management	Traditional	Traditional
Traffic Encryption	Initial	Initial
Network Resilience	Initial	Initial
Visibility and Analytics Capability	Traditional	Traditional
Automation and Orchestration Capability	Traditional	Traditional
Governance Capability	Traditional	Traditional

Source: Williams Adley's summary of CPSC and Williams Adley information

Results:
Williams Adley determined the Networks pillar to be operating at the "Traditional" and "Initial" maturity levels. The following summarizes activities completed by the CPSC related to each Networks pillar function and cross-cutting capability:

- Network Segmentation: The CPSC has deployed multiple network access and security capabilities, including cloud-based secure access services and network authentication mechanisms relying on port-based network access controls. These implementations represent meaningful progress toward strengthening user and device authentication, enforcing access control decisions closer to the resource, and reducing reliance on perimeter-based security models.
- Network Traffic Management: The CPSC has established processes for network rule and configuration changes, including those impacting mission-critical applications. Network configuration modifications are subject to an established review and approval process prior to implementation. Evidence reviewed such as audit logs and configuration documentation confirms that changes undergo manual and periodic reviews.
- Traffic Encryption: To protect information across trust boundaries, the CPSC has implemented encryption controls for both data at rest and data in transit. All network traffic accessing internal applications is encrypted, and encryption is utilized for communications with external applications to ensure confidentiality and integrity across external connections. In support of these controls, the CPSC has formalized cryptographic key management policies and implemented safeguards to protect server and service-level encryption keys.
- Network Resilience: The CPSC uses continuous health monitoring to confirm server responsiveness, application availability, and service performance. This allows failover to occur automatically before users are impacted. In addition, all Virtual Local Area Networks are configured across redundant switches connected to redundant core network components, with routing redundancy provided through standard failover protocols. This design helps ensure that failures involving network interfaces, uplinks, switches, or storage components do not interrupt service delivery.
- Visibility and Analytics Capability: The CPSC has also implemented monitoring capabilities, including centralized logging and dashboarding tools, to confirm that network traffic logs such as firewall and Intrusion Detection System/Intrusion Prevention System logs are ingested and monitored within defined requirements. Alert configurations are in place to notify appropriate CPSC personnel of critical network events, including failed authentication attempts and changes to firewall rules.
- Automation and Orchestration Capability: The CPSC employs established processes to manage the configuration and resource lifecycle across its network infrastructure and operating environments. Configuration management practices are consistently utilized to ensure systems are maintained in a controlled and standardized manner. The CPSC has also implemented Security Orchestration, Automation, and Response (SOAR) capabilities; however, these capabilities are currently operating at a manual level and are distributed across multiple platforms, including via Security Information and Event Management and

Endpoint Detection and Response tools. Advancing automation within SOAR is identified as the next step to improve operational efficiency and response effectiveness.

- Governance Capability: The CPSC has implemented static network rules through established security tools and network solutions to define baseline requirements for network access. The CPSC has also developed procedures for network governance at the access level.

3.1.4 Pillar 4: Applications and Workloads & Cross-Cutting Capabilities

The Applications and Workloads pillar ensures that applications are secure from unwanted users. To do this, agencies must make their applications available over public networks to authorized users to prevent unapproved users from accessing agency tools. ***Table 4*** below represents the CPSC's and Williams Adley's assessment of the maturity level for each function under the Applications and Workloads pillar.

Table 4 – Maturity Levels for the Applications and Workloads Pillar Functions

Function	CPSC's Self-Assessment	Williams Adley's Assessment
Application Access	Traditional	Traditional
Application Threat Protections	Initial	Initial
Accessible Applications	Initial	Initial
Secure Application Development and Deployment Workflow	Initial	Initial
Application Security Testing	Traditional	Traditional
Visibility and Analytics Capability	Traditional	Traditional
Automation and Orchestration Capability	Traditional	Traditional
Governance Capability	Initial	Initial

Source: Williams Adley's summary of CPSC and Williams Adley information

Results

Williams Adley determined the Application and Workload pillar to be operating at the "Traditional" and "Initial" maturity levels. The following summarizes activities completed by the CPSC related to each Applications and Workloads pillar function and cross-cutting capability:

- Application Access: The CPSC has established and maintains an inventory of both major and minor applications to support effective application governance and lifecycle management.
- Application Threat Protections: The CPSC has incorporated threat protection controls within mission-critical application workflows, applying defenses against known threats, and application-specific threat scenarios. The CPSC leverages web traffic analysis and filtering capabilities to detect and block malicious activity and strengthen defenses against application-level threats. In addition, the CPSC has implemented web application

protection controls to safeguard public-facing applications, including deploying multiple rule sets designed to address common and application-specific risks. These controls generate alerts when violations are detected, enabling timely awareness and response.

- Accessible Applications: The CPSC has identified mission-critical applications and has made them accessible over public networks while implementing ZT-aligned security controls. These controls include continuous security monitoring through data analysis and the enforcement of MFA to strengthen access protections across applications and workloads.
- Secure Application Development and Deployment Workflow: The CPSC provides an automated infrastructure to support development, testing, and production environments through formal code deployment processes using Continuous Integration/Continuous Deployment pipelines. Access controls are consistently implemented across these environments to support least privilege principles. The CPSC has also documented least privilege access control policies, and controls are implemented to restrict users from modifying application code within the CPSC's production environment.
- Application Security Testing: The CPSC performs application security testing prior to deployment of updates into the CPSC production environment. As part of its application security testing practices, the CPSC implements source code scanning during code uploads. These scans analyze application code for bugs, security vulnerabilities, and code quality issues.
- Visibility and Analytics Capability: The CPSC leverages IT infrastructure monitoring, management, and observability capabilities to provide insight into application performance across its environments. These capabilities are used to monitor database instances by collecting and analyzing built-in performance metrics related to system health, query execution, resource utilization, and anomalous behavior. In addition, the CPSC integrates application and performance logs with centralized security monitoring capabilities to support visibility across business units. Alerts generated from correlated performance and log data notify appropriate teams when potential performance degradation or abnormal activity is detected.
- Automation and Orchestration Capability: Application-level access is enforced through a private application access solution that segments the CPSC's applications and applies policy-based controls. Applications are grouped into defined segments, allowing access to be granted based on user roles or group membership. Within each CPSC application segment, administrators can configure access settings, including enabling or disabling client-based access as needed. Changes to application segment configurations take effect immediately, ensuring access controls are updated without delay.
- Governance Capability: The CPSC has migrated over to the CISA's Vulnerability Disclosure Policy platform. This platform enables the CPSC to safely receive, triage, manage, and remediate vulnerabilities submitted by public researchers. Additionally, the CPSC applications access is permitted primarily through authorization mechanisms and identity attributes, with role-based access controls implemented to ensure users are granted access only to applications necessary to perform their assigned job functions.

3.1.5 Pillar 5: Data & Cross-Cutting Capabilities

The Data pillar ensures that agency data is protected whenever accessed. Agencies must carefully craft and review policies related to data governance to ensure that all data security aspects are appropriately enforced across the enterprise. ***Table 5*** below represents the CPSC's and Williams Adley's assessment of the maturity level for each function under the Data pillar.

Table 5 – Maturity Levels for the Data Pillar Functions

Function	CPSC's Self-Assessment	Williams Adley's Assessment
Data Inventory Management	Traditional	Traditional
Data Categorization	Traditional	Traditional
Data Availability	Initial	Initial
Data Access	Traditional	Traditional
Data Encryption	Traditional	Traditional
Visibility and Analytics Capability	Traditional	Traditional
Automation and Orchestration Capability	Traditional	Traditional
Governance Capability	Initial	Initial

Source: Williams Adley's summary of CPSC and Williams Adley information

Results

Williams Adley determined the Data pillar to be operating at the "Traditional" and "Initial" maturity levels. The following summarizes activities completed by the CPSC related to each Data pillar function and cross-cutting capability:

- Data Inventory Management: The CPSC has implemented a centralized data lake to improve enterprise-wide data visibility. The data lake aggregates replicated data from multiple source systems and includes datasets from various organizational offices, along with associated source metadata and data owner information.
- Data Categorization: The CPSC utilizes data labeling; however, labels are applied manually at the user's discretion rather than automatically based on content inspection or matching conditions.
- Data Availability: The CPSC also has established data pipelines. Whenever a data pipeline fails an alert is triggered. The CPSC's data resides in redundant, highly available data stores hosted within a cloud-based environment. The CPSC maintains off-site backups for on-premises data, which supports data availability and recovery requirements. The CPSC utilizes industry-standard tools for its data classification and labeling policies.
- Data Access: The CPSC's access to data is primarily managed through provisioning processes. Specifically, access to file shares and databases is requested via the Helpdesk, after which users are assigned to predefined access groups. Although group structures are static, user membership within those groups is adjusted over time to accommodate changing access needs. This approach provides identity centric access control.

- Data Encryption: The CPSC implements encryption controls to protect data both at rest and in transit. Data stored within industry-standard toolsets is encrypted at rest using industry-standard encryption keys, thereby meeting baseline data protection requirements.
- Visibility and Analytics Capability: The CPSC's data is ingested from multiple sources, including system logs and output but the CPSC is still maturing its ability to monitor and analyze data feeds.
- Automation and Orchestration Capability: The CPSC implements data lifecycle and security policies including access control, data usage, storage, encryption, configuration management, backups, categorization, and sanitization primarily through manual processes.
- Governance Capability: The CPSC has defined high-level data policies and relies primarily on manual segmented implementation.

4.0 CONCLUSION AND SUGGESTIONS

Williams Adley determined that the CPSC met the "Traditional" and "Initial" maturity levels as detailed in the above sections for all ZT pillar functions and cross-cutting capabilities based on the capabilities observed at the time of assessment and validated against the ZTMM criteria.

Inquiries of personnel within EXIT confirmed to Williams Adley that initial plans and technical capabilities have begun to be implemented in order for the CPSC to achieve "Advanced" maturity for a number of ZT pillar functions and supporting cross-cutting capabilities. These plans include future enhancements intended to strengthen continuous verification, policy enforcement, and enterprise visibility, in alignment with the ZTMM and federal cybersecurity modernization objectives. Although it is important to note that under the ZTMM there is no mandated target maturity level, such as "Advanced" or "Optimal," that agencies are required to achieve, progressing to "Advanced" maturity would indicate that the CPSC has more fully operationalized ZT principles in support of risk-based access and decision making and implemented a more mature and capable ZT program.

As detailed in the Zero Trust Overview, the ZTMM serves as a strategic framework and roadmap to help agencies assess current capabilities and track progress over time. The ZTMM is intended to be used iteratively, enabling agencies to measure incremental progress and identify gaps as ZT capabilities evolve. Advancing toward more mature ZT capabilities offers demonstrable value to agencies that are able to achieve higher levels of implementation maturity. Potential benefits of mature ZT implementation include improved risk-based decision making, stronger governance and oversight, increased visibility across the enterprise, and a measurable reduction in cyber risk. In addition, Williams Adley believes that a continued emphasis on maturity progression and periodic re-assessment using the ZTMM will support the CPSC's broader cybersecurity modernization objectives and strengthen its long-term security posture.

Therefore, to support the continued maturation of the CPSC's ZT implementation, Williams Adley issued two suggestions related to strengthening the accuracy, completeness, and regularity of

the CPSC's ZT self-assessment. The CPSC last completed a ZT self-assessment in February 2024. Without a reoccurring self-assessment process, maturity determinations may no longer reflect the CPSC's current operating environment as technologies, processes, and risks change. Although Williams Adley did not conduct procedures to identify missing information within the CPSC's self-assessment, Williams Adley believes that maintaining an up-to-date and regularly performed ZT self-assessment will improve visibility into implemented controls, support effective governance and executive oversight, and reduce the risk that undocumented capabilities or processes are not consistently monitored or maintained.

In addition, although EXIT is responsible for implementing ZT requirements, effective and mature implementation of ZT controls will require continued collaboration with other offices within the CPSC that own business processes, systems, and data critical to mission operations. Establishing a repeatable and collaborative self-assessment process will help ensure these stakeholders are consistently engaged and that ZT responsibilities are shared across the enterprise. This collaboration, combined with regular updates to the CPSC's ZT self-assessment, will strengthen accountability, preserve institutional knowledge, and enable sustained maturity of the ZT program. Furthermore, a continued emphasis on performing and updating the self-assessment on a recurring basis will enable the CPSC to focus on operational effectiveness across the full range of ZT pillars and cross-cutting capabilities, support more informed prioritization of future ZT investments, reduce cyber risk, and sustain measurable progress toward a mature ZTA.

In order for the CPSC to mature its ZT implementation, Williams Adley suggests the following:

1. The CPSC perform an updated Zero Trust Maturity Model self-assessment to reflect its current Zero Trust implementation state and evolving infrastructure.

2. The CPSC implement policy that requires regular updates to the Zero Trust Maturity Model self-assessment to help ensure that Zero Trust controls are not only implemented but are operating effectively across the enterprise, thereby reducing the risk of control degradation, resource misalignment, or gaps in coverage.

APPENDIX A: SCOPE AND METHODOLOGY

A.1 Objective

The objective of this audit was to perform an assessment of the CPSC's implementation of ZT requirements and its associated pillars in accordance with OMB memorandum M-22-09, NIST SPs, and ZTMM Version 2.0 and associated internal controls.

A.2 Scope and Methodology

Williams Adley conducted procedures from September 2025 to March 2026 auditing the period of activities performed through September 2025. Williams Adley assessed the CPSC's implementation across all five ZT pillars and their corresponding functions. Our test plan was based on the CPSC's self-assessment and was specifically designed to validate whether the requirements associated with the CPSC's self-assigned maturity levels were met.

Williams Adley's test plan detailed a series of procedures designed to assess alignment with federal cybersecurity directives and best practices. Specifically, Williams Adley:

- Obtained and inspected the ZT implementation plan, submitted to the OMB and CISA in accordance with M-22-09.
- Obtained and inspected self-assessments from the CPSC to determine the accuracy of the presumed maturity on CISA's ZTMM Version 2.0.
- Performed walkthroughs, interviews, and observations with the CPSC personnel to gain a comprehensive understanding of the ZT implementation strategy, operational workflows, and supporting technologies.
- Obtained and inspected documentation, artifacts, and system-generated evidence, including screenshots of configurations and tool outputs, to assess compliance with the requirements outlined in NIST SP 800-207 and CISA's ZTMM Version 2.0.

Williams Adley 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Williams Adley provided a draft report to management on April 21, 2026, and discussed our observations and conclusions at an exit conference held on April 27, 2026.

APPENDIX B: MANAGEMENT RESPONSE

United States
Consumer Product Safety Commission

Memorandum

TO: Office of Inspector General **DATE:** April 28, 2026

FROM: Bryan Burnett
Chief Information Officer

SUBJECT: Consumer Product Safety Commission (CPSC)
Audit of the CPSC's Zero Trust Implementation
Management Response

The Office of Information and Technology Services (EXIT) thanks the Office of Inspector General (OIG) and Williams, Adley & Co. LLP for conducting an audit of CPSC's Zero Trust implementation. We appreciate the thorough assessment performed in accordance with OMB Memorandum M-22-09 and the Cybersecurity and Infrastructure Security Agency's (CISA) Zero Trust Maturity Model (ZTMM) Version 2.0. EXIT values the collaborative approach taken throughout this review and concurs with the audit results and recommendations presented.

EXIT acknowledges that Zero Trust is a multi-year modernization journey, requiring sustained effort across the agency and continuous alignment with evolving federal guidance. As noted in the report, CPSC has established foundational Zero Trust capabilities across all pillars and has begun implementing the technical and governance controls necessary to support more advanced maturity in future phases.

EXIT remains committed to strengthening the agency's cybersecurity posture and progressing along the Zero Trust maturity continuum.

Regarding the audit recommendations:

1. EXIT agrees to perform updated Zero Trust self-assessments to ensure maturity determinations remain accurate, comprehensive, and reflective of the current operating environment.

2. EXIT agrees to establish and implement a policy requiring recurring Zero Trust self-assessments, supporting continuous improvement, effective governance, and sustained accountability across the enterprise.

U.S. Consumer Product Safety Commission
4330 East-West Highway
Bethesda, MD 20814
cpsc.gov

National Product Testing & Evaluation Center
5 Research Place
Rockville, MD 20850

As funding permits, EXIT will conduct periodic Zero Trust self-assessments that may evaluate all pillars collectively or focus on a subset of Zero Trust domains at one time. This phased approach reflects the iterative nature of Zero Trust adoption and ensures that assessments remain actionable and aligned with available resources.

EXIT appreciates the OIG's partnership and insights, and we look forward to continued collaboration as we advance CPSC's Zero Trust Architecture and overall cybersecurity resilience.

APPENDIX C: ZERO TRUST PILLARS

Below is the definition as established by the ZTMM for each ZT pillar and applicable cross-cutting capability.

Identity Pillar:

The Identity pillar includes four (4) key pillar-specific functions and three (3) cross-cutting capabilities:

1. Authentication – Verifies user identity using secure, phishing-resistant MFA solutions.
2. Identity Stores – Centralized and authoritative repositories that manage user credentials, attributes, and entitlements across systems and applications.
3. Risk Assessments – Continuously evaluates user behavior, device posture, and contextual signals to inform access decisions and detect anomalies.
4. Access Management – Enforces least privilege and dynamic access policies, ensuring users access only what they need.
5. Visibility and Analytics Capability – Provides real-time monitoring and reporting on identity-related activities to detect suspicious behavior and support incident response.
6. Automation and Orchestration Capability – Integrates identity systems with other security tools to automate access provisioning, revocation, and response to identity-related threats.
7. Governance Capability – Oversees identity lifecycle processes, including onboarding, offboarding, periodic access reviews, and policy enforcement to ensure compliance and accountability.

Devices Pillar:

The Devices pillar includes four (4) key pillar-specific functions and three (3) cross-cutting capabilities:

1. Policy Enforcement & Compliance Monitoring – Ensures devices adhere to organizational security policies through continuous compliance checks and enforcement mechanisms.
2. Asset & Supply Chain Risk Management – Maintains visibility into device origin, integrity, and lifecycle risks—including third-party and supply chain vulnerabilities.
3. Resource Access – Controls which devices can access enterprise resources based on trust levels, posture, and contextual risk.
4. Device Threat Protection – Detects and mitigates malware, unauthorized access, and other threats using endpoint protection platforms and behavioral analytics.
5. Visibility and Analytics Capability – Provides real-time monitoring of device activity, posture, and anomalies to support threat detection and response.
6. Automation and Orchestration Capability – Automates device onboarding, patching, isolation, and remediation workflows to reduce manual effort and response time.
7. Governance Capability – Establishes oversight for device lifecycle management, policy enforcement, and alignment with enterprise risk management.

Networks Pillar:

The Networks pillar includes five (5) key pillar-specific functions and three (3) cross-cutting capabilities:

1. Network Segmentation – Divides networks into smaller, isolated zones to limit lateral movement and enforce least privilege access.
2. Network Traffic Management – Controls and prioritizes traffic flow based on application, user, and risk context to ensure secure and efficient communication.
3. Traffic Encryption – Ensures all internal and external traffic is encrypted using modern protocols.
4. Resource Access – Controls access to network resources based on identity, device posture, and contextual risk.
5. Network Resilience – Ensures continuity of operations through redundancy, failover mechanisms, and resistance to Denial-of-Service attacks.
6. Visibility and Analytics Capability – Provides real-time monitoring of network traffic, flows, and anomalies to detect threats and policy violations.
7. Automation and Orchestration Capability – Automates network policy enforcement, segmentation, and threat response based on telemetry and analytics.
8. Governance Capability – Establishes policies and oversight for network architecture, segmentation, encryption, and access control.

Applications and Workload Pillar:

The Applications and Workload pillar includes five (5) key pillar-specific functions and three (3) cross-cutting capabilities:

1. Application Access – Controls access to applications and workloads based on user identity, device posture, and contextual risk, enforcing least privilege.
2. Application Threat Protections – Implements runtime protections, Web Application Firewalls, and other controls to defend against common threats.
3. Accessible Applications – Ensures applications are securely accessible from any location or device, while maintaining strong access controls and session validation.
4. Secure Application Development and Deployment Workflow – Integrates security into the Software Development Lifecycle, including secure coding practices, Continuous Integration/Continuous Deployment pipeline controls, and Infrastructure-as-Code validation.
5. Application Security Testing – Conducts regular static, dynamic, and interactive testing to identify and remediate vulnerabilities before and after deployment.
6. Visibility and Analytics Capability – Monitors application behavior, access patterns, and anomalies to detect misuse, performance issues, or potential compromise.
7. Automation and Orchestration Capability – Automates application deployment, patching, and access provisioning while integrating with security tools for rapid response.
8. Governance Capability – Establishes policies and oversight for application development, access control, workload isolation, and compliance with security standards.

Data Pillar:

The Data pillar includes five (5) key pillar-specific functions and three (3) cross-cutting capabilities:

1. Data Inventory Management – Maintains a comprehensive and up-to-date inventory of all data assets, including their location, ownership, and sensitivity.
2. Data Categorization – Classifies data based on sensitivity, mission relevance, and regulatory requirements to inform access and protection strategies.
3. Data Availability – Ensures authorized users can reliably access the data they need while maintaining integrity and continuity during disruptions.
4. Data Access – Enforces access controls based on user identity, role, and contextual risk, ensuring least privilege and Just-in-Time access.
5. Data Encryption – Protects data at rest, in transit, and in use using strong encryption standards and key management practices.
6. Visibility and Analytics Capability – Monitors data access, movement, and usage patterns to detect anomalies, unauthorized activity, or potential exfiltration.
7. Automation and Orchestration Capability – Automates data classification, tagging, access provisioning, and incident response to reduce manual effort and improve consistency.
8. Governance Capability – Establishes policies and oversight for data lifecycle management, classification, retention, and compliance with legal and regulatory standards.

For more information on this report please contact us at CPSC-OIG@cpsc.gov

To report fraud, waste, or abuse, mismanagement, or wrongdoing at the CPSC go to OIG.CPSC.GOV or call (301) 504-7906

Office of Inspector General, CPSC, 4330 East-West Hwy., Suite 702, Bethesda, MD 20814