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

Audit of the CPSC's FISMA Implementation for FY 2025

August 7, 2025

25-A-04

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.

Office of Inspector General
U.S. Consumer Product Safety Commission

August 7, 2025

TO: Peter A. Feldman, Acting Chairman
Douglas Dziak, Commissioner

FROM: Christopher W. Dentel, Inspector General CHRISTOPHER DENTEL Digitally signed by CHRISTOPHER DENTEL
Date: 2025.08.07 10:18:03 -04'00'

SUBJECT: Audit of the CPSC's FISMA Implementation for 2025

The Federal Information Security Modernization Act (FISMA) requires that the U.S. Consumer Product Safety Commission's (CPSC) Office of Inspector General (OIG) annually conduct an independent evaluation of the CPSC's information security program. To assess agency compliance with FISMA and to determine the effectiveness of the information security program in 2025, we retained the services of Williams, Adley, & Co.-DC LLP (Williams Adley), an independent public accounting firm. 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 and 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.

Williams Adley assessed the CPSC's compliance with the annual FISMA reporting metrics set forth by the Department of Homeland Security and the Office of Management and Budget. They found that the CPSC had made progress in implementing FISMA requirements. The CPSC was able to close nine recommendations related to this year's in-scope Reporting Metrics. However, although improvements have occurred in a number of areas, the CPSC had still not implemented an effective information security program.

This year's FISMA report contains 16 recommendations. This includes six (6) new recommendations that are important for developing a more mature information security program. These new recommendations included two (2) recommendations from the previous year that were administratively closed and then reissued as new for 2025 to accurately reflect substantial changes or updates and ensure their ongoing significance and effectiveness. Additionally, we reissued 10 recommendations from previous FISMA evaluations. Should you have any questions about this report, please contact me at cdentel@cpsc.gov.

WILLIAMS
ADLEY

Mr. Christopher W. Dentel
Inspector General
4330 East-West Hwy,
Bethesda, Maryland, 20814

Dear Mr. Christopher Dentel

We are pleased to provide our report outlining the result of the performance audit conducted to determine the effectiveness of the U.S. Consumer Product Safety Commission's (CPSC)'s information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) for the Fiscal Year (FY) 2025 reporting period (July 1, 2024 to June 30, 2025). On January 15, 2025, the Office of Management and Budget (OMB) issued Memorandum M-25-04 ("Memorandum for the Heads of Executive Departments and Agencies: *[FY] 2025 Guidance on Federal Information Security and Privacy Management Requirements*") to provide instructions for meeting the FY 2025 FISMA reporting requirements.

To achieve this objective, we reviewed the FISMA security metrics selected by OMB and conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards* which requires that we 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 throughout the FY 2025 audit provides a reasonable basis for our conclusions and maturity ratings.

Overall, the CPSC has continued to make improvements to its overall information security program but has not met the requirements outlined within the FISMA reporting metrics to operate at an effective level of security.

CPSC management provided us with a response to the FY 2025 FISMA audit report, and it is presented in its entirety in the Management Response section of the report. Please note that we did not audit management's response and, accordingly, do not express any assurance on it.

Williams, Adley & Company-DC, LLP

August 5, 2025

Table of Contents

Abbreviations and Short Titles

BIA	Business Impact Analysis
CG	Cybersecurity Governance
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CM	Configuration Management
COOP	Continuity of Operations Plan
CP	Contingency Planning
CPSC	U.S. Consumer Product Safety Commission
C-SCRM	Cybersecurity Supply Chain Risk Management
CSF	Framework for Improving Critical Infrastructure Cybersecurity
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DPP	Data Protection and Privacy
ERM	Enterprise Risk Management
EXIT	Office of Information and Technology Services
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IDAM	Identity and Access Management
IG	Inspector General
IR	Incident Response
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan
ITSO	IT Security Office
M	Memorandum
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
RAM	Risk and Asset Management
Rev.	Revision
RMF	Risk Management Framework
SOP	Standard Operating Procedures
SP	Special Publication
ST	Security Training
Williams Adley	Williams, Adley, & Co.-DC LLP

EXECUTIVE SUMMARY

The Federal Information Security Modernization Act of 2014 (FISMA) outlines the information security management requirements for agencies. These requirements include an annual independent assessment[1] of an agency's information security program and practices. This assessment must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems and the agency's security program as a whole.

FISMA requires the annual assessment to be performed by the agency's Office of Inspector General (OIG) or by an independent external firm under OIG monitoring. The Office of Management and Budget (OMB) requires OIGs to report their responses to OMB's annual FISMA reporting questions, or metrics, for OIGs via OMB's automated data collection tool, CyberScope. In an effort to streamline the FISMA reporting process and limit the administrative burden on agencies, OMB, in conjunction with the Department of Homeland Security (DHS) and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) limited the scope of the assessment to 20 "core" and 5 supplemental Reporting Metrics in fiscal year (FY) 2025.

The U.S. Consumer Product Safety Commission (CPSC) OIG retained Williams, Adley, & Co.-DC LLP (Williams Adley, we), an independent public accounting firm, to perform the independent assessment of the CPSC's implementation of FISMA for FY 2025 and to determine the effectiveness of the CPSC's information security program. This report documents the results of the OIG's FISMA assessment which was conducted in accordance with the Government Accountability Office's *General Auditing Standards*. Specifically, we assessed the effectiveness of the CPSC's information security program against the annual Inspector General (IG) FISMA Reporting Metrics set forth by the DHS and OMB. Agency efforts are scored against a five level maturity model ranging from level one, "ad hoc," to level five, "optimized," with level four, "managed and measurable," generally considered effective.

WHAT WE FOUND

This year's FISMA assessment found that the CPSC made progress in implementing FISMA requirements. The CPSC was able to close nine recommendations related to this year's in-scope Reporting Metrics. Specifically, the CPSC:

- Defined and documented the taxonomy of the CPSC's information system components
- Implemented solutions to perform scenario analysis and modeled potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting impact to organizational systems and data
- Implemented registration and inventorying procedures for the CPSC's information systems
- Developed, documented, and implemented a process for determining and defining system boundaries
- Implemented the CPSC's policies and procedures for provisioning, managing, and reviewing privileged accounts

[1] Throughout this report, the terms 'audit' and 'assessment' are used interchangeably.

- Developed and implemented policies and procedures in support of Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*
- Performed an assessment of the knowledge, skills, and abilities of the CPSC personnel with significant security responsibilities
- Developed a security awareness and training strategy/plan
- Defined and implemented event logging requirements

In addition, the CPSC made strides in defining risk management activities. For instance, the CPSC has initiated an Enterprise Risk Management (ERM) program, slated for implementation via a phased approach. As part of this initiative, to ensure governance and accountability, the CPSC has also established the Senior Management Council co-chaired by the Deputy Executive Director for Operations Support and the Deputy Executive Director for Safety Operations. This council will provide essential oversight of management's implementation of an effective risk management framework, reinforcing the agency's commitment to proactive risk identification and mitigation. An effective ERM program is invaluable to ensure that organizational and mission objectives are integrated with and, ultimately, drive information security priorities.

However, overall, we determined that the CPSC still has not implemented an effective information security program in accordance with FISMA requirements. Specifically, the CPSC did not address all information security weaknesses identified in the OIG's previous FISMA evaluations.

In commenting on a draft version of this report, management provided responses, which are presented in Appendix B.   We did not assess management's response and, accordingly, we express no opinion on the responses.

WHAT WE RECOMMEND

We've made a total of 16 recommendations to improve the CPSC's adherence to FISMA. This includes 10 recommendations we reissued from previous FISMA evaluations. In addition, we issued six (6) new recommendations, two (2) of which are from the previous fiscal years and were administratively closed. These were reissued as new for FY 2025 to accurately reflect substantial changes or updates and ensure their ongoing significance and effectiveness. A consolidated list of recommendations related to this year's in-scope Reporting Metrics can be found at Table 5-1.

1. OBJECTIVE

The objective was to perform an independent assessment of the CPSC's implementation of FISMA and to determine the effectiveness of the information security program for fiscal year (FY) 2025.

2. BACKGROUND AND CRITERIA

The Federal Information Security Modernization Act (FISMA), signed into law by the President on December 18, 2014, superseded and reformed the 2002 Act, establishing updated information security management requirements for federal agencies. These requirements include an annual independent assessment of an agency's information security program and practices. This assessment must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems and the agency's security program as a whole.

FISMA requires the annual assessment to be performed by the agency's Office of Inspector General (OIG) or by an independent external firm under OIG monitoring. Office of Management and Budget (OMB) Memorandum (M)-25-04, *FY 2025 Guidance on Federal Information Security and Privacy Management Requirements*, requires the OIG to report their responses to OMB's annual FISMA reporting questions for OIGs via CyberScope.

Overall, we determined that the CPSC has not implemented an effective information security program and practices in accordance with FISMA requirements. Specifically, we identified 16 deficiencies across 7 domains. The deficiencies identified included the lack of an effective risk management process which was a result of the CPSC not taking a holistic approach to manage information security risks or utilizing information security resources to address previously identified deficiencies. We made six (6) new recommendations which, if implemented, would improve the CPSC's security posture. Management concurred with all of the recommendations. The previous fiscal year's open recommendations are identified within section five (5) of the report, "Consolidated List of Recommendations".

Federal Information Security Modernization Act of 2014

The requirements of the Federal Information Security Management Act of 2002 were updated with the passage of FISMA. FISMA was established to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. Specifically, FISMA requires federal agencies to develop, document, and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency. Furthermore, FISMA "emphasizes a risk-based policy for cost-effective security," underscoring the importance of agencies taking a risk-based approach to protecting their information, information systems, and addressing their unique cybersecurity challenges.

National Institute of Standards and Technology Risk Management Framework

The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) established the information security risk management best practices via the RMF as detailed in the NIST Special Publication (SP) 800-37, Revision (Rev.) 2, *RMF for Information Systems and Organizations*, and NIST SP 800-39, *Managing Information Security Risk*. The NIST RMF provides guidance for federal agencies to establish a robust enterprise-wide information security risk management program to guide the implementation of an information security program. This NIST guidance postulates that establishing effective governance and a formalized approach to information security risk management is the critical first step to achieving an effective information security program.

Key Changes to the IG FISMA Reporting Metrics in FY 2025

Williams, Adley, & Co.-DC LLP (Willams Adley) utilized the Inspector General (IG) FY 2025 FISMA Reporting Metrics published by the OMB and the Department of Homeland Security (DHS), in consultation with the Council of the Inspectors General on Integrity and Efficiency (CIGIE), to evaluate the effectiveness of the CPSC's information security program and practices. Reflecting OMB's shift in emphasis away from compliance in favor of risk management, IGs are encouraged to evaluate the IG metrics based on the risk tolerance and threat model of their agency and to focus on the practical security impact of weak control implementations, rather than strictly evaluating from a view of compliance or the mere presence or absence of controls. Section V of OMB's M-25-04 indicates that OMB has selected a core group of metrics, representing a combination of administration priorities and other highly valuable controls, that must be evaluated annually. The remainder of the standards and controls are evaluated on a biennial cycle based on a calendar agreed to by CIGIE, the Chief Information Security Officer Council, OMB, and the Cybersecurity and Infrastructure Agency (CISA), beginning in FY 2023.

According to the IG FISMA[2] Reporting Metrics, one of the goals of the annual FISMA assessment is to assess agency progress toward achieving outcomes that strengthen federal cybersecurity, including implementing the administration's priorities and best practices. The FY 2025 IG FISMA Reporting Metrics focused on 20 core and 5 supplemental IG metrics and did not include the full suite of 66 metrics. The core IG FISMA Reporting Metrics were chosen based on alignment with Executive Order 14028, *Improving the Nation's Cybersecurity*, as well as recent OMB guidance to agencies. The IG FISMA Reporting Metrics have been updated to determine agency progress in achieving the objectives, as follows:

- NIST published CSF Version 2.0 which highlights the critical role governance plays in managing cybersecurity risks and incorporating cybersecurity into an organization's broader Enterprise Risk Management (ERM) strategy. As such, a new IG FISMA function (Govern) has been created that includes a new domain (Cybersecurity Governance). In addition, new supplemental metrics are designed to assess the maturity of an organizations:

[2] OMB, DHS, CIGIE, "*FY 2025 IG FISMA Reporting Metrics*"

    - Use of cybersecurity profiles to understand, tailor, assess, prioritize and communicate cybersecurity objectives.
    - Cybersecurity risk management strategy, which establishes an organization's priorities, constraints, risk tolerance and appetite statements, and is used to support operational risk decisions.
    - Processes and authorities to foster cybersecurity accountability, performance assessment, and continuous improvement.

- In addition, to align with the CSF 2.0, the Supply Chain Risk Management domain moved from the Identify function to the Govern function and was renamed to Cybersecurity Supply Chain Risk Management (C-SCRM) to better reflect the cybersecurity environment. Furthermore, the metrics renamed a domain in the Identify function (Risk and Asset Management vs. Risk Management) to group metrics on system inventory and hardware, software, and data management.

- Lastly, the updated metrics align with new NIST guidance related to Zero Trust Architecture[3] implementation. Specifically, the FY 2025 IG FISMA Reporting Metrics include two new supplemental metrics that are critical to achieving Zero Trust Architecture objectives. These new metrics assess the maturity of an organization's:
    - Data management capabilities.
    - Ability to monitor and measure the integrity and security posture of all owned and associated assets.

Cybersecurity Framework

In response to the growing concern related to cybersecurity, Executive Order 13636[4] was issued which requires the development of a set of industry standards and best practices to help organizations manage information security risks to combat cybersecurity challenges. As a result of the executive order, NIST released the *Framework for Improving Critical Infrastructure Cybersecurity* (CSF) on February 12, 2014. The CSF[5] provides guidelines for organizations to protect critical infrastructure[6] by using business drivers to direct information security activities. This approach requires management to consider information security risks as part of the organization's comprehensive risk management processes.

To emphasize the importance of protecting critical infrastructure, Executive Order 13800[7] was issued to hold agency heads accountable for managing cybersecurity risk in their organizations. Specifically, Executive Order 13800 requires agency heads to lead integrated teams of senior

[3] https://zerotrust.cyber.gov/downloads/M-22-09%20Federal%20Zero%20Trust%20Strategy.pdf

[4] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013.

[5] CSF 2.0 was published in February 26, 2024.

[6] According to Executive Order 13636, critical infrastructure is defined as "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

[7] Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 11, 2017.

executives with expertise in information technology, security, budgeting, acquisition, law, privacy, and human resources. Furthermore, Executive Order 13800 requires agency heads to use the CSF to manage the agency's cybersecurity risk and holds agency heads accountable for ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes.

In 2024, NIST released the CSF 2.0 which provides federal agencies with an updated common structure for identifying and managing information security risks across the enterprise and provides guidance for assessing the maturity of controls established to address those risks. The latest CSF now contains six information security functions that give federal agencies the ability to select and prioritize improvements in information security risk management. The six information security functions are as follows:

- **Govern** – The Govern function requires aligning cybersecurity efforts with the organization's overall mission, objectives, and risk management strategy. Its purpose is to ensure that cybersecurity is not just a technical IT function, but an integral part of the organization's enterprise-wide risk management and business operations.
- **Identify** – The Identify function requires the development of organizational understanding to manage information security risk to systems, assets, data, and capabilities. The activities in the Identify function are foundational for effective implementation of the CSF. Understanding the business context, the resources that support critical functions, and the related information security risks enable an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.
- **Protect** – The Protect function requires the development and implementation of appropriate safeguards to ensure delivery of critical services, and limit and contain the impact of a potential cybersecurity event.
- **Detect** – The Detect function requires the development and implementation of appropriate activities to timely discover the occurrence of a cybersecurity event.
- **Respond** – The Respond function requires the development and implementation of appropriate activities to take regarding a detected cybersecurity event and contain the impact of a potential cybersecurity event.
- **Recover** – The Recover function requires the development and implementation of appropriate activities to maintain plans for resilience and to timely restore any capabilities or services that were impaired because of a cybersecurity event.

FY 2025 IG FISMA Reporting Metrics

The FY 2025 IG FISMA Reporting Metrics identified 20 core metrics and 5 supplemental metrics developed by OMB, DHS, and CIGIE and incorporated the NIST Framework's six (6) information security functions into its ten (10) defined security domains as follows:

1. Govern Function (Cybersecurity Governance and Cybersecurity Supply Chain Risk Management)
2. Identify Function (Risk and Asset Management)

3. Protect Function (Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training)
4. Detect Function (Information Security Continuous Monitoring)
5. Respond Function (Incident Response)
6. Recover Function (Contingency Planning)

1. Govern Function

- *Cybersecurity Governance –* An agency with a Cybersecurity Governance (CG) program clearly defines its mission, stakeholder expectations (internal and external), and all relevant legal, regulatory, and contractual requirements related to cybersecurity. Cybersecurity risks are treated as core business risks, on par with financial, reputational, or operational risks and are integrated into the organization's broader ERM strategy.
- *Cybersecurity Supply Chain Risk Management* – An agency with an effective C-SCRM ensures that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and C-SCRM requirements and reports qualitative and quantitative performance measures on the effectiveness of its C-SCRM program.

2. Identify Function

- *Risk and Asset Management –* An agency with an effective Risk and Asset Management (RAM) program maintains an accurate inventory of information systems, hardware assets, and software assets; consistently implements its risk management policies, procedures, plans, and strategies at all levels of the organization; as well as monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its risk management program.

3. Protect Function

- *Configuration Management –* An agency with an effective Configuration Management (CM) program employs automation to maintain an accurate view of the security configurations for all information system components connected to the agency's network; consistently implements its CM policies, procedures, plans, and strategies at all levels of the organization; centrally manages its flaw remediation process; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its CM program.
- *Identity and Access Management* – An agency with an effective Identity and Access Management (IDAM) program ensures that all privileged and non-privileged users utilize strong authentication to organizational systems; employs automated mechanisms to support the management of privileged accounts; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its IDAM program.
- *Security Training* – An agency with an effective Security Training (ST) program identifies and addresses security knowledge, skills, and abilities gaps; measures the effectiveness of its security awareness and training program; and ensures staff are consistently collecting, monitoring, and analyzing qualitative and quantitative

performance measures on the effectiveness of security awareness and training activities.

- *Data Protection and Privacy* – An agency with an effective Data Protection and Privacy (DPP) program maintains confidentiality, integrity, and availability of its data and is able to assess its security and privacy controls as well as its breach response capacities and reports on qualitative and quantitative DPP performance measures.

4. **Detect Function**
   - *Information Security Continuous Monitoring* – An agency with an effective Information Security Continuous Monitoring program (ISCM) maintains ongoing authorizations of information systems; integrates metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM policies, procedures, plans, and strategies.

5. **Respond Function**
   - *Incident Response* – An agency with an effective Incident Response (IR) program utilizes profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents; manages and measures the impact of successful incidents; uses IR metrics to measure and manage the timely reporting of incident information to organizational officials and external stakeholders; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures on the effectiveness of its IR policies, procedures, plans, and strategies.

6. **Recover Function**
   - *Contingency Planning* – An agency with an effective Contingency Planning (CP) program establishes contingency plans; employs automated mechanisms to thoroughly and effectively test system contingency plans; communicates metrics on the effectiveness of recovery activities to relevant stakeholders; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures on the effectiveness of information system CP program activities.

In addition, based on the IG FISMA Reporting Metrics, OIGs are required to assess the effectiveness of information security programs on a maturity model spectrum, in which the foundational levels ensure that agencies develop sound policies and procedures, and the advanced levels capture the extent that agencies institutionalize those policies and procedures. Maturity is to be determined based on a five-level scale (Level 1 to Level 5). The maturity model score of Level 4 (Managed and Measurable) is considered to be an effective level of security at the metric, domain, function, and overall program level. Please see additional details of the five levels of the maturity model spectrum below:

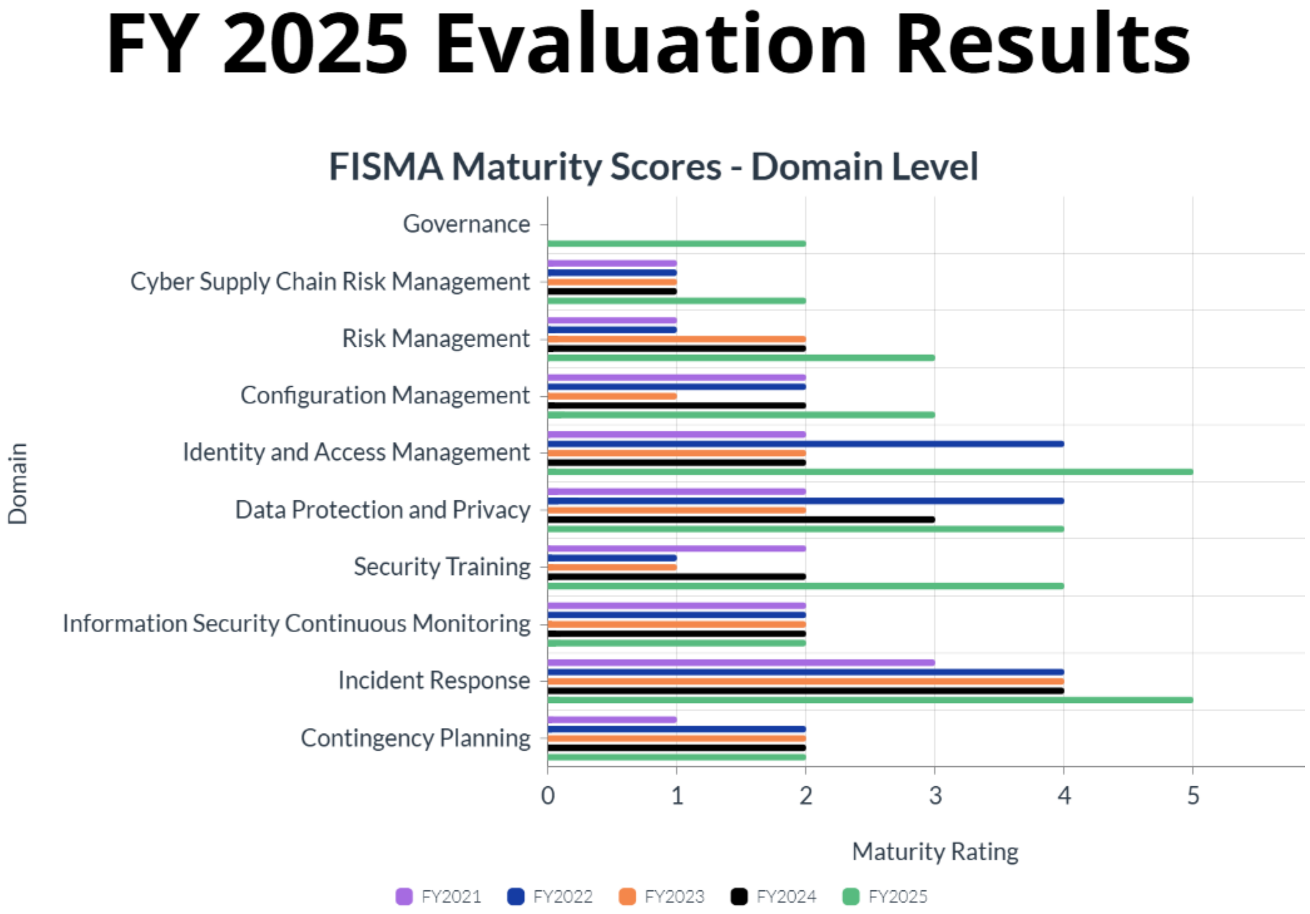
- **Level 1: Ad-hoc** – Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.

- **Level 2: Defined** – Policies, procedures, and strategies are formalized and documented but not consistently implemented.
- **Level 3: Consistently Implemented** – Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
- **Level 4: Managed and Measurable** – Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
- **Level 5: Optimized** – Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Williams Adley utilized the criteria established by the federal government to assess the CPSC's FY 2025 information security program in accordance with FISMA. For a complete listing of criteria, please refer to Appendix A.3.

3. ASSESSMENT RESULTS

Based on the IG FISMA Reporting Metrics requirements, we concluded that the CPSC has made improvements to its information security program and made progress in implementing some of the recommendations from previous FISMA assessments; however, the CPSC has not implemented an effective information security program in FY 2025.



**Please note that questions change from year to year. Thus, results across years are not directly comparable.*

Figure 1. FY 2025 Assessment Results

4. FINDING: The CPSC Has Not Implemented an Effective Information Security Program

Overall, Williams Adley determined that the CPSC has not implemented an effective information security program and practices in accordance with FISMA requirements. During the assessment, Williams Adley identified deficiencies for seven of the related IG FISMA metric domains. The results for all functions and domains are documented in the sections below.

Root Cause

The CPSC information security program was not effective because the CPSC still has not fully developed and implemented a comprehensive approach to managing information security risks or to effectively utilize information security resources to address previously identified information security deficiencies. Explicit guidance and processes to address information security risks and integrate those risks into the broader agency-wide ERM program have not been developed. Therefore, the CPSC’s ERM program remains largely ineffective.

Williams Adley has reported the lack of an effective ERM program since FY 2020. While the Office of Information Technology Services (EXIT) is responsible for managing and implementing much of the CPSC’s information security program and related practices, the overall responsibility for the ERM program resides with CPSC executive management. Throughout the CPSC, including executive management, there has been high turnover in key positions, which may have caused delays in implementation. In 2025, EXIT began to receive specific direction from CPSC executive management about how to integrate information security risk into the organization-wide risk management practices.

Effect

The ineffective CPSC security program has led to data breaches in the past, and could again in the future, leading to personally identifiable information, financial information, and other sensitive information becoming compromised. It is critical that the agency implement an effective information security program to protect data that is stored, processed, and/or transmitted by the CPSC. Sensitive information at the CPSC includes trade secrets, personal health information, and other proprietary business information, which, if compromised, could potentially expose the CPSC to a loss of consumer and industry trust and lead to significant financial losses for the businesses involved.

Williams Adley believes that information security risks are a key business risk, and thus, the implementation of an effective information security program needs to be prioritized. Further, without an effective information security program, the CPSC mission to keep consumers safe will remain at risk.

Recommendations

The CPSC must address the individual conditions presented in the applicable IG FISMA metric domains to create an effective information security program. Below we have provided a list of recommendations associated with identified conditions. A majority of the recommendations (10) identified below are directly related to prior year deficiencies and recommendations (see Table 5-1), while six (6) of the recommendations identified below are new this year as indicated by the parenthetical reference "(*2025 recommendation*)."

4.1 Govern Function Area

Progress

The CPSC has begun to establish a CG program in alignment with the IG FISMA Reporting Metrics and NIST CSF 2.0 by drafting key documentation such as a cybersecurity profile. Concurrently, the CPSC has made some updates to its ERM program. These updates include:

i. The recruitment of a risk management specialist which would enhance the capabilities for effective risk identifications and mitigations.
ii. The formal designation of the Chief Financial Officer and the Deputy Executive Director for Operations Support to serve as ERM leadership, providing essential executive oversight and strategic direction.
iii. The initiation of a phased ERM implementation approach, which would leverage CPSC's internal control framework as a structured basis for integration.
iv. The formalization of a Senior Management Council with oversight responsibilities for the implementation of an effective risk management framework.

The CPSC has also made progress towards addressing the previously identified C-SCRM deficiencies. For example, the CPSC has drafted a C-SCRM Strategy and Plan and C-SCRM Implementation Plan. However, the C-SCRM documents provided remain in draft.

Cybersecurity Governance Results

Williams Adley determined that the CPSC was operating at **Maturity Level 2 – Defined** for the CG IG FISMA metric domain. Without a defined and maintained target profile, the CPSC may lack a clear roadmap to achieve its desired cybersecurity outcomes, which could hinder strategic planning, resource allocation, and progress tracking.

Williams Adley identified the following deficiencies within the CG IG FISMA metric domain:

i. The CPSC has not finalized the draft policies and procedures for developing and maintaining current and target cyber security profiles.
ii. The CPSC has not finalized the draft risk management strategy that identifies and defines the following:
    - Enterprise priorities, constraints, risk tolerance, appetite statements and assumptions.
    - Risk management objectives that are established and agreed to by enterprise stakeholders.
    - Established and defined lines of communication for risks, including risks from suppliers and third parties.
    - Roles and responsibilities.

Cybersecurity Supply Chain Risk Management Results

Williams Adley determined that the CPSC was operating at **Maturity Level 2 – Defined** for the C-SCRM IG FISMA metric domain. Without effectively implementing a comprehensive C-SCRM process at all levels of the organization, the CPSC may be unable to address the root causes associated with existing cybersecurity supply chain risks. By not taking strategic steps to identify and assess risks within the agency's supply chain, unknown risks may be introduced by products, system components, systems, and services of external providers.

Williams Adley identified the following deficiencies within the C-SCRM IG FISMA metric domain:

i. The CPSC has not finalized procedures and processes to ensure that the CPSC-defined products, system components, systems, and services adhere to its cybersecurity and C-SCRM requirements.

Govern Function Recommendations

We recommend that the CPSC:

1. Finalize and implement policies and procedures for creating and maintaining current and target cybersecurity profiles in alignment with NIST CSF Guidance. (*Cybersecurity Governance 2025 Recommendation*).
2. Finalize and implement a comprehensive Risk Management Strategy that defines roles and responsibilities, enterprise risk priorities, objectives, and communication protocols, including third-party risk considerations. (*Cybersecurity Governance 2025 Recommendation*).

4.2 Identify Function Area

Progress

The CPSC has demonstrated progress in addressing previously identified recommendations regarding RAM. Specifically, the CPSC has established key procedural documents, including an Information System Registration, Inventory and Assessment Standard Operating Procedure (SOP) and an Information Technology Security Operations Minor Application Assessment SOP. By accomplishing these efforts, the CPSC has successfully implemented its registration and inventory procedures for information systems. Further to enhance its asset management capabilities, the CPSC maintains hardware and software inventories through asset discovery tool sets. In terms of cybersecurity oversight, the CPSC has deployed a solution that provides a centralized view of cybersecurity activities. This is supported by the utilization of technologies for trend analysis, scenario analysis, and the modeling of potential responses. Furthermore, as a foundational element of this program, the CPSC has completed a risk register, which delineates the severity, likelihood, and overall risk level associated with each identified risk.

Risk and Asset Management Results

Williams Adley determined that the CPSC was operating at **Maturity Level 3 – Consistently Implemented** for the RAM IG FISMA metric domain. Without effectively implementing a comprehensive RAM process at all levels of the organization, the CPSC may be unable to address the root causes associated with existing information security risks. In addition, without an effective risk management process in place the CPSC cannot ensure the information security efforts align with the CPSC's mission and organizational priorities. Furthermore, the absence of finalized and enforceable data governance policies means the agency lacks a cohesive framework for the consistent and secure management of its data assets.

Williams Adley identified the following deficiencies within the RAM IG FISMA metric domain:

i. The CPSC has not finalized and implemented the Information Security Risk Management procedures or an Information Security Risk Management Strategy that defines the elements below in accordance with the latest NIST risk management guidance:
   - Scope and associated processes of the risk management strategy at each CPSC tier (e.g., at the enterprise, business process, and information system levels).
   - Roles and responsibilities of key personnel.
   - The CPSC information security risk profile, risk appetite, and risk tolerance, as applicable.
   - The CPSC's processes and methodologies for framing, assessing categorizing, responding to, addressing, and monitoring information security.
   - Processes for communication of the risk management strategy across the CPSC.
   - The technology utilized to support the CPSC's information security program.

ii. The CPSC has not finalized and implemented how information security risks are communicated to all necessary internal and external stakeholders and has not defined how quickly these risks must be communicated.

iii. The CPSC has not finalized and implemented the roles and responsibilities of the internal and external stakeholders involved in its risk management processes, which is necessary to support a holistic information security risk management program and ERM program.

iv. The CPSC's has not developed and implemented policies and procedures related to data governance.

Identify Function Recommendations

We recommend that the CPSC:

3. Continue to develop and implement an Enterprise Risk Management (ERM) program based on National Institute of Standards and Technology and ERM Playbook (Office of Management and Budget Circular A- 123, Section II requirement) guidance (*Risk and Asset Management 2025 Recommendation*).
4. Develop and implement policies and procedures for developing and maintaining a comprehensive and accurate inventory of data and corresponding metadata for the CPSC's data types. (*Risk and Asset Management 2025 Recommendation*).

4.3 Protect Function Area

Progress

The CPSC has made progress on open prior year CM recommendations. The CPSC has developed Vulnerability Management SOPs to address vulnerabilities identified by CISA Binding Operational Directive 22-01, focusing on the remediation of known exploited vulnerabilities. In addition, the CPSC has developed an IT Security Office Security Configuration Baseline Management Plan and related SOPs for common secure configuration baselines. Further, the CPSC is actively working towards implementing secure configurations in alignment with the Defense Information System Agency Security Technical Implementation Guide benchmarks. Moreover, the CPSC is also actively working on integrating and leveraging DHS Continuous Diagnostics and Mitigation capabilities.

The CPSC has achieved an effective maturity rating for its IDAM program. The CPSC has made great progress in addressing previously identified IDAM deficiencies. For example, the CPSC has identified and documented potentially incompatible duties permitted by privileged accounts. Furthermore, the CPSC logs and actively monitors activities performed while using privileged access that permits potentially incompatible duties. Lastly, the CPSC has implemented policies and procedures for provisioning, managing, and reviewing privileged accounts. The CPSC possesses a strong and effective IDAM, demonstrating strong controls over who can access its information systems and data. The CPSC also implemented multifactor authentication mechanisms.

The CPSC has also achieved an effective maturity rating for its DPP domain. Specifically, EXIT is currently working on a project that enhances the Data Loss Prevention (DLP) tool capabilities. For example, EXIT has implemented firewall rules to block certain websites and categories of websites, data loss prevention rules to monitor unencrypted emails that contain sensitive data, and some DLP rules to protect and prevent unauthorized transmissions.

Lastly, the CPSC has also achieved an effective maturity rating for its ST domain. The CPSC has developed its Awareness and Training policy and its Security and Privacy Training Plan. The CPSC has performed an assessment of the knowledge, skills, and abilities of CPSC personnel with significant security responsibilities. Furthermore, the CPSC tracks individuals who have been identified as having significant security or privacy responsibilities and assigns and tracks annual role-based security training.

Configuration Management Results

Williams Adley determined that the CPSC was operating at **Maturity Level 3 – Consistently Implemented** for the CM IG FISMA metric domain. An effective CM program is critical to identify and mitigate vulnerabilities that can be exploited within the CPSC's environment. By not taking the strategic steps to implement proper secure configurations, unknown risks and vulnerabilities may be introduced by new or existing products, system components, systems, and services of external providers.

Williams Adley identified the following deficiencies within the CM IG FISMA metric domain:

i. The CPSC has not yet fully implemented the configuration settings/common secure configurations for its information systems.

Identity and Access Management Results

Williams Adley determined that the CPSC was operating at **Maturity Level 5 - Optimized** for the IDAM IG FISMA metric domain. Williams Adley did not identify any conditions or provide any formal recommendations related to the CPSC's IDAM program. Effective IDAM controls are critical for preventing unauthorized access to CPSC's information systems. Important identity management practices are essential to ensure that only approved and authorized personnel can access sensitive data and resources, thereby safeguarding the integrity, confidentiality, and availability of the CPSC's information. The CPSC should continue to prioritize and optimize its IDAM processes.

Data Protection and Privacy Results

Williams Adley determined that the CPSC was operating at **Maturity Level 4 – Managed and Measurable** for the DPP IG FISMA metric domain. Although the CPSC achieved an overall effective maturity rating for DPP, the CPSC must address existing deficiencies to fully achieve an effective DPP program. An effective DPP program is critical to protect personally identifiable information and other sensitive data, as well as prevent data loss.

Williams Adley identified the following deficiencies within the DPP IG FISMA metric domain:

i. The CPSC has not fully implemented a DLP tool.

Security Training Results

Williams Adley determined that the CPSC was operating at **Maturity Level 4 – Managed and Measurable** for the ST IG FISMA metric domain. Williams Adley did not identify any conditions or provide any formal recommendations related to the CPSC's ST program. The CPSC has maintained its progress toward implementing an effective ST program which is critical to protecting the confidentiality, integrity, and availability of systems and data. The CPSC has addressed its identified knowledge, skills, and abilities gaps through trainings. The CPSC's ST program currently demonstrates effectiveness in meeting the foundational requirements outlined by FISMA and its supporting NIST guidance. Personnel are clearly receiving valuable information regarding their security responsibilities, contributing significantly to the agency's overall security posture. The CPSC should continue to advance its security trainings in alignment with FISMA's emphasis on continuous improvement—it is imperative to continuously refine and mature the program's processes. This proactive approach will ensure that the training remains relevant and impactful as new FISMA requirements emerge, and the threat landscape evolves.

Protect Function Recommendations

We recommend that the CPSC:

5. Fully implement, assess, and maintain secure configuration settings in accordance with defined configuration management policy and security configuration baseline procedures (*Configuration Management 2025 recommendation*).

4.4 Detect Function

Progress

The CPSC last authorized its major systems in September 2023. Recently, the CPSC began updating its ISCM plan, Information System Registration, Inventory and Assessment Procedures, and Minor Application Assessment Procedures.

Information Security Continuous Monitoring Results

Williams Adley determined that the CPSC was operating at **Maturity Level 2 – Defined** for the ISCM IG FISMA metric domain. Information system resources are essential to an organization's success; therefore, it is critical that these systems are monitored to ensure implemented security controls remain effective and provide active management and monitoring of risks. By not taking the steps to develop and implement proper ISCM policies and procedures and integrate those processes with organizational risks, the CPSC will not be able to maintain an effective security posture.

Williams Adley identified the following deficiencies within the ISCM IG FISMA metric domain:

i. The CPSC's System and Information Integrity Policy and the Communications Protection Policy is not up to date. Specifically, these policies were last revised in 2017 and contain obsolete language that needs to be updated in accordance with the NIST Special SP 800-53, Rev. 5, published in September 2020.

ii. The ISCM Program is not designed in accordance with the NIST guidance to support each organizational tier, specifically the business process and enterprise-wide tiers. For example, according to NIST SP 800 37 (Rev.2): Task P-7, the organizational continuous monitoring strategy must address monitoring requirements at the organizational level and mission/business process level. In addition, according to NIST SP 800-137: Sections 3.1 and 3.2, the ISCM program should provide clear visibility into organizational assets and leverage threat information. This guidance also requires the ISCM strategy to be based on organizationally defined risk tolerances and to consider business/mission impacts; however, no evidence was provided to demonstrate that this was done.

iii. System Security Plans include information that is out-of-date and no longer applicable. For example, we determined that the General Support System Local Area Network System Security Plan contains information regarding minor applications which were all last assessed in 2015, 2016, and 2017, and are based on the NIST security control catalog that is out-of-date.

Detect Function Recommendations

We recommend that the CPSC:

6. Update all relevant Information Security Continuous Monitoring policies, procedures, and supporting documentation based on latest National Institute of Standard and Technology guidance (*ISCM 2025 recommendation).*

4.5 Respond Function

Progress

In FY 2025, the CPSC continued to make progress in implementing an effective IR program. For example, the CPSC has implemented additional tool sets and obtained licenses to implement event logging requirements, and therefore fulfill OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, compliance requirements.

Incident Response Results

Williams Adley determined that the CPSC was operating at **Maturity Level 5 – Optimized** for the IR IG FISMA metric domain. Williams Adley did not identify any conditions or provide any formal recommendations related to the CPSC's IR program. Williams Adley noted that this is the fourth consecutive year that the CPSC's IR program has been rated at effective levels. An effective IR program is critical for detecting, identifying, containing, eradicating, and recovering from security incidents. Overall, Williams Adley determined that the CPSC's IR program exceeds the requirements for an effective IR program. The CPSC has established an effective IR program that capably handles security events. To ensure sustained security and adapt to the dynamic threat landscape, it is prudent to continue to be proactive in optimizing current tools and integrating necessary updates to enhance the program's capabilities.

4.6 Recover Function

Progress

The CPSC took a step towards addressing previously identified CP deficiencies. Specifically, the CPSC has conducted Information System Contingency Plan (ISCP) testing for its major information systems.

Contingency Planning Results

Williams Adley determined that the CPSC was operating at **Maturity Level 2 – Defined** for the CP IG FISMA metric domain. Information system resources are essential to an organization's success; therefore, it is critical that services provided by these systems operate effectively and do so without excessive interruption. An effective CP program is critical for the recovery of the CPSC's operations in the event of a disaster or an outage. An outdated and incomplete CP program increases the possibility of disruption and confusion, as well as limiting the CPSC's opportunity to return to normal operations.

Williams Adley identified the following deficiencies within the CP IG FISMA metric domain:

i. The CPSC did not include all necessary information into its Continuity of Operations Plan (COOP) or integrated its COOP and organizational-level Business Impact Analyses (BIAs) with its system-level BIAs or its ISCP. For example:
   - The system-level BIAs and ISCPs were developed prior to (and independently from) the COOP and organization-level BIAs, therefore, the COOP and organization-level BIAs were not used to support those efforts.
   - Although statutory requirements are listed in the COOP, it is not clear what business processes or systems support those requirements, which is important when defining recovery priorities and tasks.
   - It is not clear in the COOP or organizational BIAs which systems support Mission Essential Functions and which systems are necessary for essential supporting activities; this is an important factor when defining recovery priorities and tasks.
   - Essential records in the COOP are not listed beyond a few examples, and when requested, a list of essential records was not available.

ii. System-level BIAs are out-of-date.

iii. The CPSC does not employ automated mechanisms to test ISCPs.

Recover Function Recommendations

We identified no new recommendations for FY 2025. All reissued prior year recommendations related to this year's in-scope IG FISMA Reporting Metrics for the Recover Function can be found at Table 5-1.

5. CONSOLIDATED LIST OF RECOMMENDATIONS

Table 5-1: Index of Recommendations: includes new and prior-year recommendations in-scope for the FY 2025 IG FISMA Reporting Metrics.

Function	No.	Recommendation
Govern	**Newly Issued Recommendations**	
	25-01	Finalize and implement policies and procedures for creating and maintaining current and target cybersecurity profiles in alignment with National Institute of Standards and Technology Cybersecurity Framework Guidance (*Cybersecurity governance 2025 Recommendation*).
	25-02	Finalize and implement a comprehensive Risk Management Strategy that defines roles and responsibilities, enterprise risk priorities, objectives, and communication protocols, including third-party risk considerations (*Cybersecurity governance 2025 Recommendation*).
	Re-Issued Prior Year Recommendations	
	21-13	Finalize and implement supply chain risk management procedures to ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain risk management requirements (*Cybersecurity Supply Chain Risk Management 2021 Recommendation).*
Identify	**Newly Issued Recommendations**	
	25-03	Continue to develop and implement an Enterprise Risk Management program based on National Institute of Standards and Technology and Enterprise Risk Management Playbook (Office of Management and Budget Circular A- 123, Section II requirement) guidance (*Risk and Asset Management 2025 Recommendation*).
	25-04	Develop and implement policies and procedures for developing and maintaining a comprehensive and accurate inventory of data and corresponding metadata for the Consumer Product Safety Commission data types. (*Risk and Asset Management 2025 Recommendation*).
	Re-Issued Prior Year Recommendations	
	21-07	Finalize and implement a formal strategy to address information security risk management requirements as prescribed by the National Institute of Standard and

Function	No.	Recommendation
		Technology guidance (*Risk and Asset Management 2020 recommendation).*
	21-08	Complete an assessment of information security risks related to the identified deficiencies and document a corresponding priority listing to address identified information security deficiencies and their associated recommendations. A corrective action plan should be developed that documents the priorities and timing requirements to address these deficiencies *(Risk and Asset Management 2020 recommendation).*
Protect	**Newly Issued Recommendations**	
	25-05	Fully implement, assess, and maintain secure configuration settings in accordance with defined configuration management policy and security configuration baseline procedures *(Configuration Management 2025 recommendation).*
	Re-Issued Prior Year Recommendations	
	22-04	Fully implement a data loss prevention solution *(Data Protection and Privacy 2020 recommendation - modified).*
Detect	**Newly Issued Recommendations**	
	25-06	Update all relevant Information Security Continuous Monitoring policies, procedures, and supporting documentation based on latest National Institute of Standard and Technology guidance (*Information Security Continuous Monitoring 2025 recommendation*).
	Re-Issued Prior Year Recommendations	
	21-39	Establish and implement a strategy for identifying and integrating organizational risk tolerance and mission risk tolerances into the Information Security Continuous Monitoring program, and ensure the Information Security Continuous Monitoring supporting plan, policy, and procedures are updated to consider each program tier (*Information Security Continuous Monitoring 2020 Recommendation - modified*).
	22-03	Update the System Security Plans to include the most up-to-date information and assess the relevant minor applications (*Information Security Continuous Monitoring 2022 recommendation).*
Recover	**Re-Issued Prior Year Recommendations**	
	21-45	Update the Continuity of Operations Plan, or other documentation supporting Consumer Product Safety

Function	No.	Recommendation
		Commission’s contingency planning efforts, to provide traceability from the statutory requirements to the mission essential functions and to include all necessary information, for example: (1) a list of systems that support the Mission Essential Functions, (2) a list of systems necessary for essential supporting activities, and (3) a list of records essential for the Consumer Product Safety Commission’s continuity of operations (*Contingency Planning 2020 recommendation - modified*).
	21-46	Integrate documented contingency plans with the newly developed Continuity of Operations Plan and organizational Business Impact Analyses *(Contingency Planning 2020 recommendation - modified*).
	23-14	Develop and implement policies and procedures for maintaining a Continuity of Operations Plan and conducting organizational and system level Business Impact Analyses in accordance with current federal guidance (e.g., National Institute of Standards and Technology Special Publication 800-34/53, Department of Homeland Security *Federal Continuity Directive 1*, National Institute of Standards and Technology Cybersecurity Framework , and National Archives and Records Administration guidance) (*Contingency Planning 2023 recommendation*).
	24-02	Perform a cost benefit analysis of introducing automation to support the testing of system contingency plans; and apply the appropriate risk mitigation strategy (*Contingency Planning 2024 recommendation*).

Appendix A: Objective, Scope and Methodology

A.1 Objective

The objective was to perform an independent assessment of the CPSC's implementation of FISMA[8] for FY 2025. In support of this objective, Williams Adley conducted the assessment in accordance with OMB M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*.

A.2 Scope

The assessment focused on reviewing the CPSC's implementation of FISMA for FY 2025 based on OMB M-25-04. The FISMA assessment covered the period of July 1, 2024, to June 30, 2025. The assessment included determining the effectiveness of the CPSC's enterprise-wide information security policies, procedures, and practices; and a review of information security policies, procedures, and practices of a representative subset of the CPSC's information systems, including contractor systems and systems provided by other federal agencies.

A.3 Methodology

We performed qualitative analyses to assess the effectiveness of the CPSC's efforts to secure its information systems. The audit included an assessment of the NIST CSF Function Levels, as specified in the FY 2025 IG FISMA Reporting Metrics:

- Govern (Cybersecurity Governance)
- Govern (Cybersecurity Supply Chain Risk Management)
- Identify (Risk and Asset Management)
- Protect (Configuration Management)
- Protect (Identity and Access Management)
- Protect (Data Protection and Privacy)
- Protect (Security Training)
- Detect (Information Security Continuous Monitoring)
- Respond (Incident Response)
- Recover (Contingency Planning)

FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or source. To ensure the adequacy and effectiveness of these controls, FISMA requires an independent external review of the information security program. The FY 2025 IG FISMA Reporting Metrics developed by the OMB, DHS, and CIGIE are intended to provide guidance on the OIG annual assessments, as required by FISMA, 44 U.S.C. 3555(j).

[8] Public Law. No. 113-283, FISMA, December 18, 2014.

Williams Adley performed this audit from March through July 2025 and 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 its 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.

To perform this assessment, we interviewed CPSC senior management and employees to assess managerial effectiveness and operational controls in accordance with federal guidance. We remotely observed the CPSC's operations, obtained evidence to support our conclusions and recommendations, tested effectiveness of established or defined controls, conducted sampling where applicable, and collected and reviewed written documents to supplement observations and interviews.

Use of Computer-Processed Data

During the assessment, Williams Adley used computer-processed data to obtain samples and information regarding the existence of information security controls. For example, Williams Adley requested a system generated list of incidents for FY 2025 for testing. The list was used to support the assessment procedures in the Incident Response IG FISMA metric domain. Williams Adley assessed the reliability of the computer-generated data primarily by comparing selected data with source documentation, data from prior years, inquiring with CPSC personnel, and observing the selected data being generated. Where applicable, Williams Adley determined that the information was sufficiently reliable for assessing the adequacy of related information security controls.

Sampling Methodology

With respect to the sampling methodology employed, standards indicate that either a statistical or judgmental sample can yield sufficient and appropriate evidence. Based on professional judgement, Williams Adley did not use statistical sampling during this assessment. Williams Adley employed another type of sample permitted by standards—namely, a non-statistical sample known as a judgmental sample. A judgmental sample is a sample selected by using discretionary criteria rather than criteria based on the laws of probability.

In this assessment, Williams Adley has taken great care in determining the criteria to use for sampling based on Williams Adley's judgement of risk. For all samples selected during the assessment, Williams Adley used non-statistical sampling techniques where applicable and appropriate. As guidance, Williams Adley used the American Institute of Certified Public Accountants, *Audit Guide Audit Sampling*.[9] This guidance assists in applying sampling methodology in accordance with auditing standards. Moreover, Williams Adley used, whenever practicable, random numbers to preclude the introduction of any bias in sample selection although a non-statistical technique was used. Williams Adley acknowledges that it is possible that the information security deficiencies identified in this report may not be as prevalent or may

[9] American Institute of Certified Public Accountants *Audit Guide*, *Audit Sampling*, March 1, 2014.

not exist in other information systems that were not tested.

Assessment, testing, and analysis were performed in consideration with guidance from the following:

I. 44 U.S. Code Section 3511 – Data Inventory and Federal Data Catalogue
II. Center for Internet Security (CIS) Top 18 Security Controls: Control 13
III. CIS Critical Security Controls v8: 10.1
IV. CIS Critical Security Controls v8: 8.11
V. CIS Critical Security Controls: 3.2
VI. CIS Top 18 Security Controls: Control 11
VII. CIS Top 18 Security Controls: Control 15
VIII. CIS Top 18 Security Controls: Control 3, 9, and 10
IX. Cybersecurity and Infrastructure Security Agency (CISA) Operational Guidance
X. CISA Zero Trust Maturity Model
XI. CISA Cybersecurity Incident Response Playbooks
XII. DHS Binding Operational Directive 18-01
XIII. DHS Binding Operational Directive 18-02
XIV. DHS Binding Operational Directive 23-01
XV. DHS Emergency Directive 19-01
XVI. DHS's ICT Supply Chain Library
XVII. Executive Order 13800
XVIII. Executive Order 14028
XIX. Federal Continuity Directive-1
XX. Federal Continuity Directive-2
XXI. Federal Information Processing Standard 199
XXII. Federal Records Act
XXIII. Federal Zero Trust Data Security Guide
XXIV. FISMA 2014
XXV. FY 2025 Chief Information Officer FISMA Metrics: 2.1, 2.1.1, 2.2, and 10.8
XXVI. FY 2025 Chief Information Officer FISMA Metrics: 8.1, 8.2, and 8.3
XXVII. NIST SP 800- 34 (Rev. 1): Section 3.2
XXVIII. NIST CSF v2.0: DE.AE-02
XXIX. NIST CSF v2.0: DE.CM-09
XXX. NIST CSF v2.0: GV.0C-01, GV.0C-02, GV.0C-03, GV.0C-04, GV.0C-05
XXXI. NIST CSF v2.0: GV.0V-01, GV.0V-02, GV.0V-03
XXXII. NIST CSF v2.0: GV.RM-01, GV.RM-02, GV.RM-03, GV.RM-04, GV.RM-06
XXXIII. NIST CSF v2.0: GV.SC-01, GV.SC-02, GV.SC-03, GV.SC-04, GV.SC-05, GV.SC-06, GV.SC-07
XXXIV. NIST CSF v2.0: ID.AM-07
XXXV. NIST CSF v2.0: ID.IM-02, ID.IM-04
XXXVI. NIST CSF v2.0: ID.RA-01, ID.RA-04, ID.RA-05, ID.RA-06
XXXVII. NIST CSF v2.0: PR.DS-02, PR.DS-11, ID.AM-08, and DE.CM-01
XXXVIII. NIST CSF v2.0: PR.PS-01
XXXIX. NIST CSF v2.0: Section 3.1
XL. NIST Federal Information Processing Standards 200

XLI. NIST Interagency or Internal Report 8179

XLII. NIST Internal Report 8286

XLIII. NIST Internal Report 8286A, 8286B, 8286C, and 8286D

XLIV. NIST Security Measures for Executive Order-Critical Software Use: SM 2.3, SM 2.4, SM 3.3, SM 4.2 and SM 4.3

XLV. NIST SP 800- 137: Sections 3.1 and 3.6

XLVI. NIST SP 800- 171 Rev. 3

XLVII. NIST SP 800- 207: Section 2.1

XLVIII. NIST SP 800- 39

XLIX. NIST SP 800-152

L. NIST SP 800-161 (Rev.1)

LI. NIST SP 800-218: Task PO.1.3 NIST IR 8276

LII. NIST SP 800-37 (Rev. 2): Task P-7, P-2, P-3, P-14, R-2, R-3, P-10 and P-16

LIII. NIST SP 800-53 (Rev. 5) : AC-4, CA-3, CA-7, CM-8, CM-10, CM-11, CM-12, CM-13, PM-5, PM-9, RA-2, RA-3, CM-3, CM-6, CM-7, RA-5, SI-2, SI-3, PM-6, PM-14, PM-31, AU-12, SC-34, SC-35, SI-4, SI-7, SA-4. SA-9, SR-3. SR-5, SR-6, SC-3, SC-8, SC-28, MP-3, MP-6, and SI-12(3), SI 7(8), SI-4(4)(18), SC-7(10), SC-18, PM-9, PM-28, PM-1, PM-11, RA-7, CP-2, CP-3, CP-4 and RA-9

LIV. NIST SP 800-70 and 800-40 (Rev. 4)

LV. OMB Circular A-130

LVI. OMB M-16-17

LVII. OMB M-19-03

LVIII. OMB M-21-31

LIX. OMB M-22-01

LX. OMB M-22-18

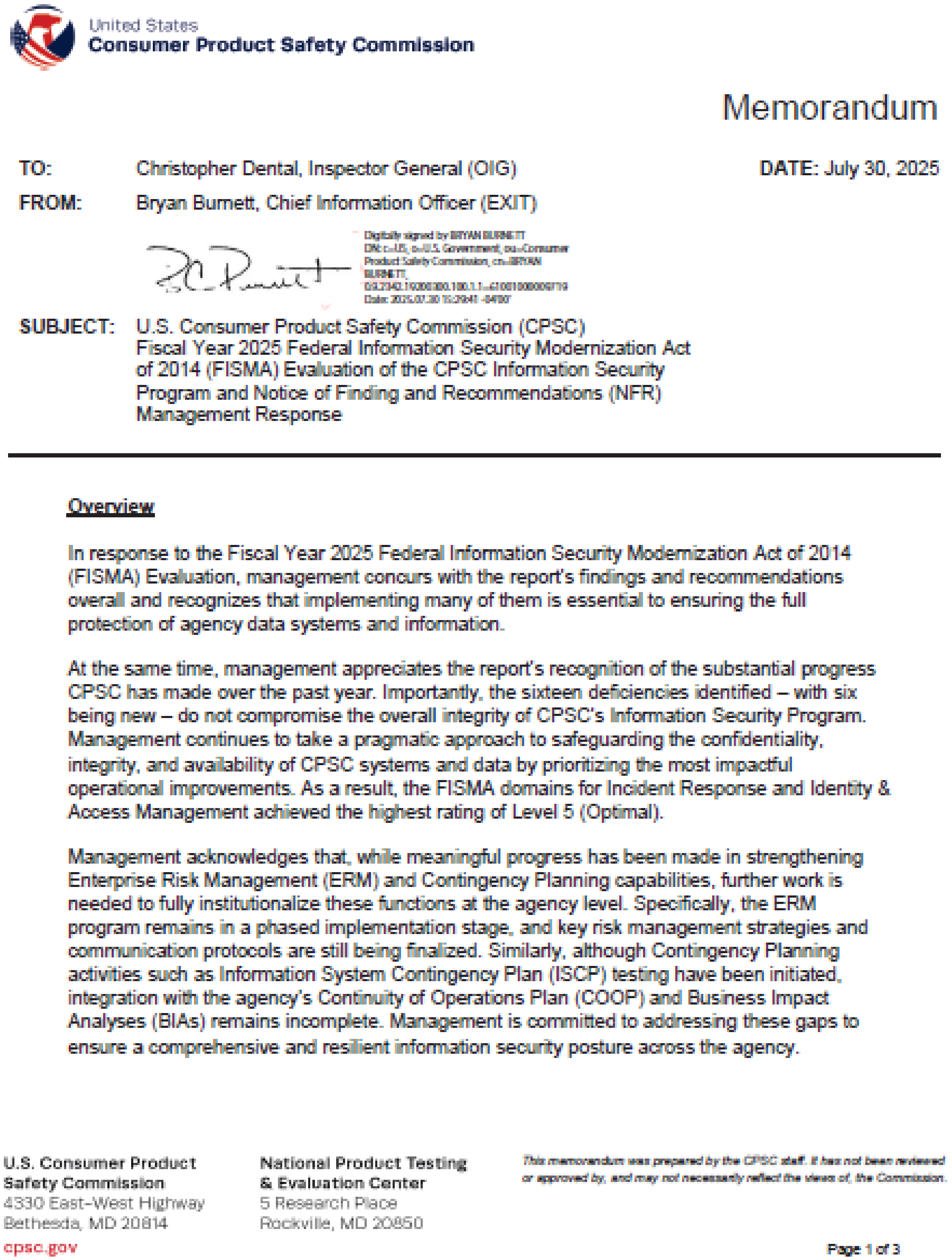
LXI. OMB M-25-04

LXII. Privacy Act of 1974

LXIII. Public Law 113-283

LXIV. The Federal Acquisition Supply Chain Security Act of 2018

Appendix B: Management Response



United States
Consumer Product Safety Commission

Memorandum

TO: Christopher Dental, Inspector General (OIG)

DATE: July 30, 2025

FROM: Bryan Burnett, Chief Information Officer (EXIT)

Digitally signed by BRYAN BURNETT
DN: c=US, o=U.S. Government, ou=Consumer Product Safety Commission, cn=BRYAN BURNETT, 0.9.2342.19200300.100.1.1=61001000009719
Date: 2025.07.30 15:29:41 -04'00'

SUBJECT: U.S. Consumer Product Safety Commission (CPSC) Fiscal Year 2025 Federal Information Security Modernization Act of 2014 (FISMA) Evaluation of the CPSC Information Security Program and Notice of Finding and Recommendations (NFR) Management Response

Overview

In response to the Fiscal Year 2025 Federal Information Security Modernization Act of 2014 (FISMA) Evaluation, management concurs with the report's findings and recommendations overall and recognizes that implementing many of them is essential to ensuring the full protection of agency data systems and information.

At the same time, management appreciates the report's recognition of the substantial progress CPSC has made over the past year. Importantly, the sixteen deficiencies identified – with six being new – do not compromise the overall integrity of CPSC's Information Security Program. Management continues to take a pragmatic approach to safeguarding the confidentiality, integrity, and availability of CPSC systems and data by prioritizing the most impactful operational improvements. As a result, the FISMA domains for Incident Response and Identity & Access Management achieved the highest rating of Level 5 (Optimal).

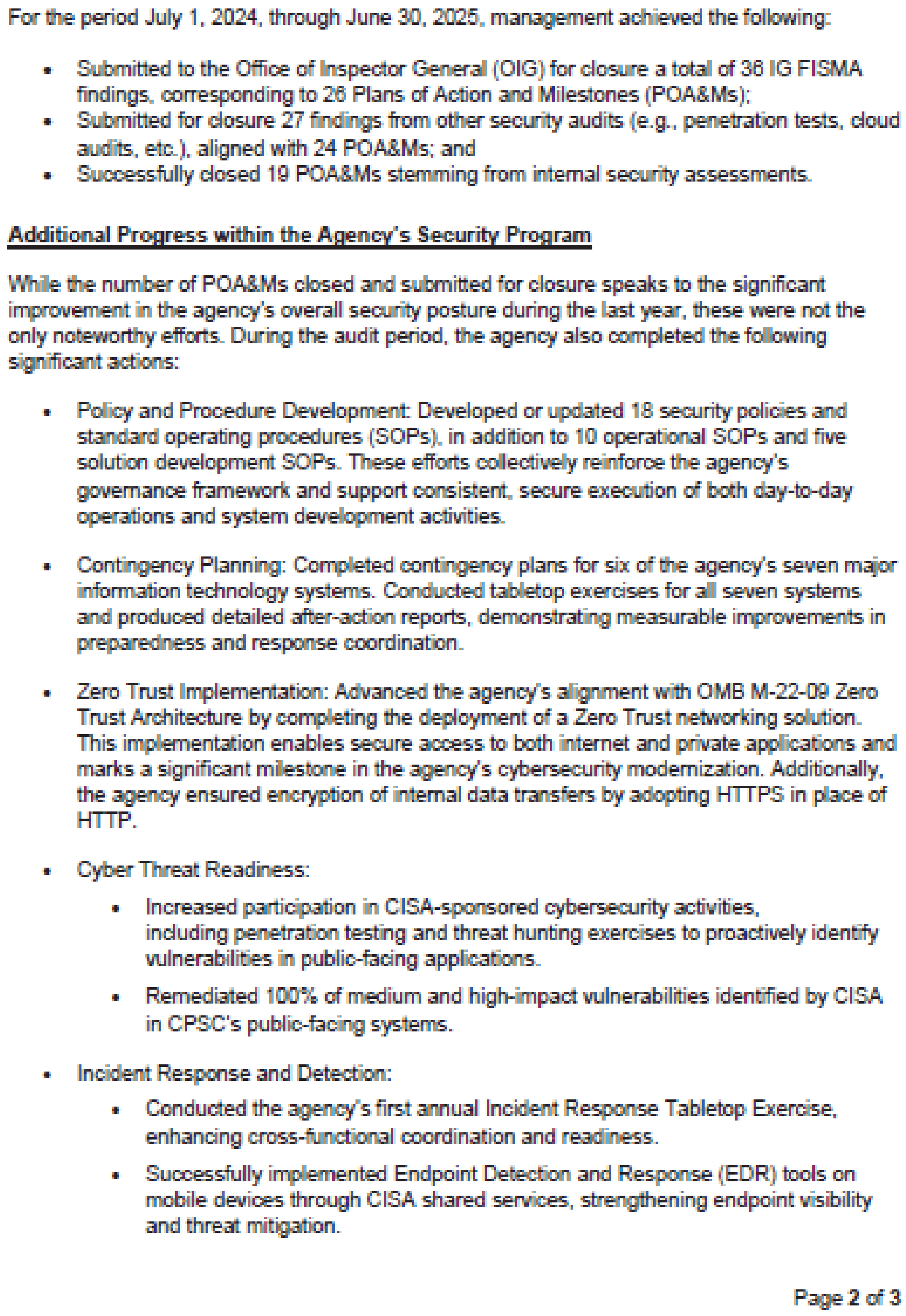
Management acknowledges that, while meaningful progress has been made in strengthening Enterprise Risk Management (ERM) and Contingency Planning capabilities, further work is needed to fully institutionalize these functions at the agency level. Specifically, the ERM program remains in a phased implementation stage, and key risk management strategies and communication protocols are still being finalized. Similarly, although Contingency Planning activities such as Information System Contingency Plan (ISCP) testing have been initiated, integration with the agency's Continuity of Operations Plan (COOP) and Business Impact Analyses (BIAs) remains incomplete. Management is committed to addressing these gaps to ensure a comprehensive and resilient information security posture across the agency.

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

This memorandum was prepared by the CPSC staff. It has not been reviewed or approved by, and may not necessarily reflect the views of, the Commission.

Page 1 of 3



For the period July 1, 2024, through June 30, 2025, management achieved the following:

- Submitted to the Office of Inspector General (OIG) for closure a total of 36 IG FISMA findings, corresponding to 26 Plans of Action and Milestones (POA&Ms);
- Submitted for closure 27 findings from other security audits (e.g., penetration tests, cloud audits, etc.), aligned with 24 POA&Ms; and
- Successfully closed 19 POA&Ms stemming from internal security assessments.

Additional Progress within the Agency's Security Program

While the number of POA&Ms closed and submitted for closure speaks to the significant improvement in the agency's overall security posture during the last year, these were not the only noteworthy efforts. During the audit period, the agency also completed the following significant actions:

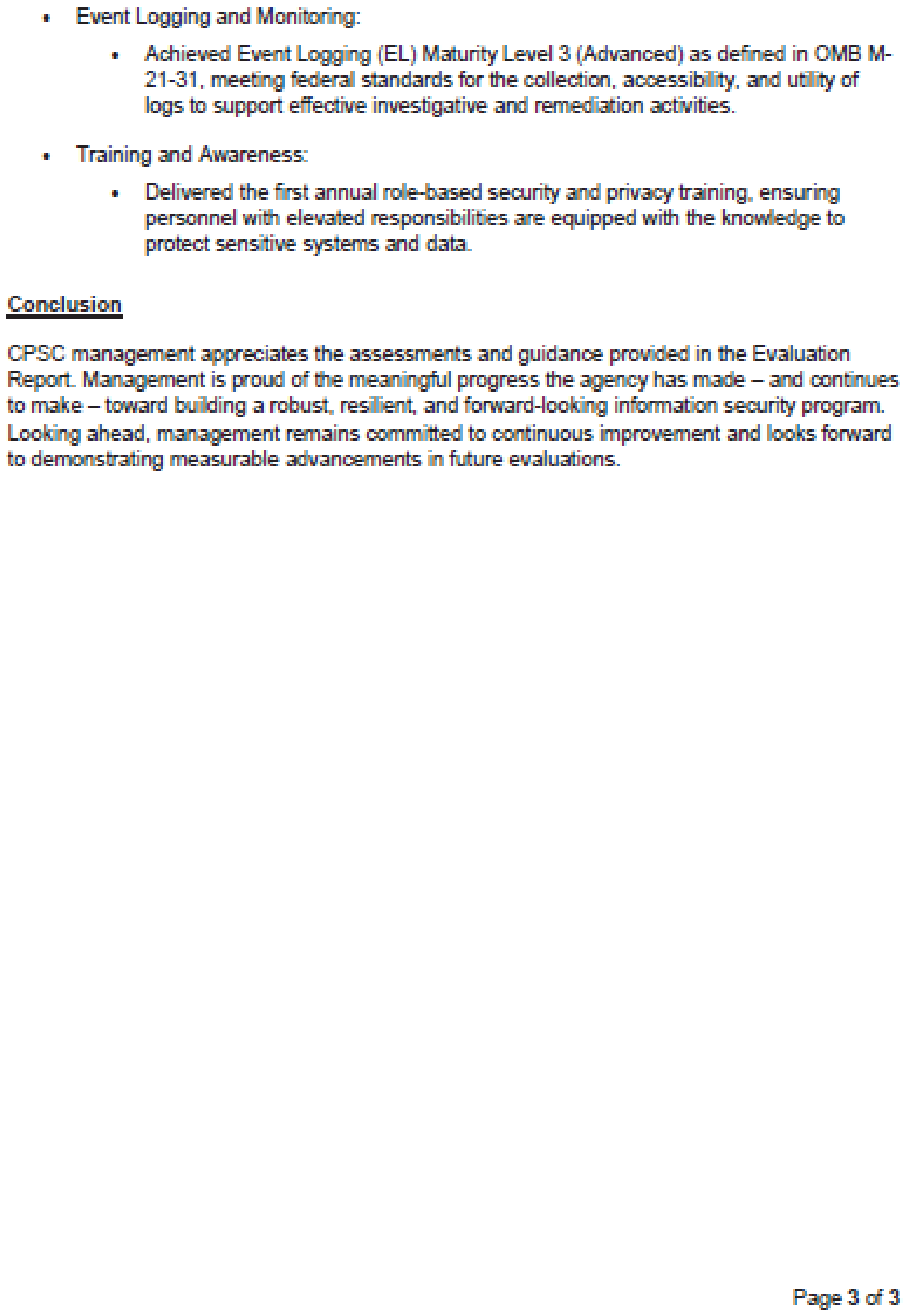
- Policy and Procedure Development: Developed or updated 18 security policies and standard operating procedures (SOPs), in addition to 10 operational SOPs and five solution development SOPs. These efforts collectively reinforce the agency's governance framework and support consistent, secure execution of both day-to-day operations and system development activities.

- Contingency Planning: Completed contingency plans for six of the agency's seven major information technology systems. Conducted tabletop exercises for all seven systems and produced detailed after-action reports, demonstrating measurable improvements in preparedness and response coordination.

- Zero Trust Implementation: Advanced the agency's alignment with OMB M-22-09 Zero Trust Architecture by completing the deployment of a Zero Trust networking solution. This implementation enables secure access to both internet and private applications and marks a significant milestone in the agency's cybersecurity modernization. Additionally, the agency ensured encryption of internal data transfers by adopting HTTPS in place of HTTP.

- Cyber Threat Readiness:
  - Increased participation in CISA-sponsored cybersecurity activities, including penetration testing and threat hunting exercises to proactively identify vulnerabilities in public-facing applications.
  - Remediated 100% of medium and high-impact vulnerabilities identified by CISA in CPSC's public-facing systems.

- Incident Response and Detection:
  - Conducted the agency's first annual Incident Response Tabletop Exercise, enhancing cross-functional coordination and readiness.
  - Successfully implemented Endpoint Detection and Response (EDR) tools on mobile devices through CISA shared services, strengthening endpoint visibility and threat mitigation.



- Event Logging and Monitoring:
  - Achieved Event Logging (EL) Maturity Level 3 (Advanced) as defined in OMB M-21-31, meeting federal standards for the collection, accessibility, and utility of logs to support effective investigative and remediation activities.
- Training and Awareness:
  - Delivered the first annual role-based security and privacy training, ensuring personnel with elevated responsibilities are equipped with the knowledge to protect sensitive systems and data.

Conclusion

CPSC management appreciates the assessments and guidance provided in the Evaluation Report. Management is proud of the meaningful progress the agency has made – and continues to make – toward building a robust, resilient, and forward-looking information security program. Looking ahead, management remains committed to continuous improvement and looks forward to demonstrating measurable advancements in future evaluations.

Page 3 of 3

Office of Inspector General • U.S. Consumer Product Safety Commission •

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