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

Evaluation of the CPSC's FISMA Implementation for FY 2024

July 30, 2024

24-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.

July 30, 2024

TO: Alexander Hoehn-Saric, Chairman
Peter A. Feldman, Commissioner
Richard L. Trumka Jr., Commissioner
Mary T. Boyle, Commissioner
Douglas Dziak, Commissioner

FROM: Christopher W. Dentel, Inspector General CHRISTOPHER DENTEL

Digitally signed by CHRISTOPHER DENTEL
Date: 2024.07.30 16:11:49 -04'00'

SUBJECT: Evaluation of the CPSC's FISMA Implementation for FY 2024

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 for fiscal year 2024, 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 evaluation. The contract required that the evaluation be performed in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) *Quality Standards for Inspection and Evaluation* (QSIE). 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 CIGIE's QSIE.

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, although improvements have occurred in some areas, the CPSC had still not implemented an effective information security program. Establishing effective governance and a formalized approach to managing information security risk is the critical first step to achieving an effective information security program. This is a step the CPSC has still not taken despite its lack of an effective Enterprise Risk Management program having been cited by this office as a Top Agency Management and Performance Challenge every year for over a decade.

This year's FISMA report contains 35 recommendations. The CPSC closed eight of the prior years' recommendations, three new recommendations were made, and 32 recommendations from prior years remain open. Should you have any questions about this report, please contact me.

Table of Contents

Abbreviations and Short Titles

BIA	Business Impact Analysis
BOD	Binding Operational Directive
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CISA	Cybersecurity and Infrastructure Security Agency
COOP	Continuity of Operations Plan
CPSC	U.S. Consumer Product Safety Commission
Cybersecurity Framework	Framework for Improving Critical Infrastructure Cybersecurity
DHS	Department of Homeland Security
DPP	Data Protection and Privacy
EL	Event Logging
ERM	Enterprise Risk Management
EXIT	Office of Information and Technology Services
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IAM	Identity and Access Management
IG	Inspector General
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan
M	Memorandum
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
Rev.	Revision
RMF	Risk Management Framework
SCRM	Supply Chain Risk Management
SP	Special Publication
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 evaluation of an agency's information security program and practices. This evaluation 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 evaluation 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 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 evaluation to 20 "core" and 17 supplemental reporting metrics in fiscal year (FY) 2024.

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 evaluation of the CPSC's implementation of FISMA for FY 2024 and to determine the effectiveness of its information security program. This report documents the results of the OIG's FISMA evaluation. Specifically, we assessed the CPSC's compliance with 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 evaluation found that the CPSC made progress in implementing FISMA requirements. The CPSC was able to close eight recommendations. Specifically, the CPSC:

- established and implemented policies and procedures to manage software licenses using automated monitoring and expiration notifications
- established and implemented a policy and procedure to ensure that only authorized hardware and software execute on the agency's network
- developed, implemented, and disseminated a current configuration management policy which is in accordance with the most recent National Institute of Standards and Technology (NIST) guidance
- identified and documented the characteristics of items that are to be placed under Configuration Management control
- developed and implemented a Configuration Management plan to ensure it includes all requisite information
- identified and documented potentially incompatible duties permitted by privileged accounts

- logged and actively monitored activities performed while using privileged access that permits potentially incompatible duties
- tested the set of documented contingency plans

However, we determined that the CPSC has not implemented an effective information security program in accordance with FISMA requirements. The CPSC still does not have a formal approach to information security risk management and did not prioritize addressing all of the information security weaknesses identified in the OIG's previous FISMA evaluations. The CPSC reviewed open findings and prioritized remediation efforts based on personnel workloads, impact on information technology infrastructure, and availability of workforce. However, the CPSC Office of Information and Technology Services (EXIT) currently has two open security positions that have not been filled due to a hiring freeze which impacted the progress on addressing previously identified weaknesses. This lack of staff in combination with the lack of an Enterprise Risk Management (ERM) program and guidance from CPSC senior management on how to integrate information security risk management hinders the further development of the information security program. An effective ERM program is invaluable to ensure that organizational and mission objectives are integrated with and, ultimately, drive information security priorities.

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

WHAT WE RECOMMEND

To improve the CPSC's implementation of FISMA, we made 35 recommendations that the CPSC must address in order to mature its information security program. We provided three (3) new recommendations and reissued 32 prior recommendations related to the specific deficiencies identified.

1. OBJECTIVE

The objective was to perform an independent evaluation of the CPSC’s implementation of FISMA and to determine the effectiveness of the information security program for FY 2024.

2. BACKGROUND AND CRITERIA

On December 18, 2014, the president signed FISMA, which reformed the Federal Information Security Management Act of 2002. FISMA outlines the information security management requirements for agencies. These requirements include an annual independent evaluation of an agency’s information security program and practices. This evaluation 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 evaluation to be performed by the agency’s OIG or by an independent external firm under OIG monitoring. OMB Memorandum (M)-24-03, *Fiscal Year 2024 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. We identified deficiencies in each of the in-scope IG FISMA domains. Specifically, we identified 35 deficiencies across 9 domains. Key deficiencies included a lack of an effective risk management process which resulted from the CPSC not taking a holistic approach to manage information security risks or utilize information security resources to address previously identified deficiencies.

We made 35 recommendations which, if implemented, would improve the CPSC’s security posture. Management concurred with all of the recommendations. Please note, the majority of our recommendations (32) carried over from previous years; however, we made three (3) new 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

NIST established the information security risk management best practices via the Risk Management Framework (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.

Cybersecurity Framework

In response to the growing concern related to cybersecurity, Executive Order 13636[1] 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* (Cybersecurity Framework) on February 12, 2014. The Cybersecurity Framework[2] provides guidelines for organizations to protect critical infrastructure[3] 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[4] 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 executives with expertise in information technology, security, budgeting, acquisition, law, privacy, and human resources. Furthermore, Executive Order 13800 requires agency heads to use the Cybersecurity Framework 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.

The Cybersecurity Framework provides federal agencies with a 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 Cybersecurity Framework contains five information security functions that give federal agencies the ability to select and prioritize improvements in information security risk management. The five information security functions are as follows:

- **Identify –** The identify function requires the development of organizational understanding

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

[2] Version 1.1 of the Cybersecurity Framework was published in April 2018 to provide refinements, clarifications, and enhancements to Version 1.0 published in February 2014.

[3] 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."

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

to manage information security risk to systems, assets, data, and capabilities. The activities in the identify function are foundational for effective implementation of the Cybersecurity Framework. 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 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.

The five functions (identify, protect, detect, respond, and recover) of the Cybersecurity Framework provide agencies with the structure and guidance to improve their information security program by using an effective risk management strategy to manage and protect their environment. Furthermore, these functions require the use of risk management processes to enable organizations to inform and prioritize decisions regarding information security. The five functions support recurring risk assessments and validation of business drivers to help agencies implement the necessary information security activities that reflect desired outcomes. Each function places reliance on the development of those functions preceding it. For example, an organization cannot *protect* its information technology environment effectively without first *identifying* its key information systems and the risks faced by each. Moreover, an organization cannot *respond* to cybersecurity events if it has not first implemented proper measures to *detect* them.

FY 2023-FY 2024 Inspector General FISMA Reporting Metrics

The FY 2024 IG FISMA Reporting Metrics identified 20 core metrics and 17 supplemental metrics developed by OMB, DHS, and CIGIE and incorporated the NIST Framework's five (5) information security functions into its nine (9) previously defined security domains as follows:

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

1. Identify Function

○ *Risk Management* - An agency with an effective risk management 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.

○ *Supply Chain Risk Management* - An agency with an effective Supply Chain Risk Management (SCRM) ensures that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and SCRM management requirements and reports qualitative and quantitative performance measures on the effectiveness of its SCRM program.

2. Protect Function

○ *Configuration Management* – An agency with an effective configuration management 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 configuration management 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 configuration management program.

○ *Identity and Access Management* – An agency with an effective Identity and Access Management (IAM) 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 Identity, and Access Management program.

○ *Security Training* – An agency with an effective security training 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.

3. Detect Function

○ *Information Security Continuous Monitoring* – An agency with an effective Information Security Continuous Monitoring (ISCM) program 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.

4. Respond Function

○ *Incident Response* – An agency with an effective incident response 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 incident response 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 incident response policies, procedures, plans, and strategies.

5. Recover Function

○ *Contingency Planning* – An agency with an effective contingency planning 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 contingency planning program activities.

In addition, based on the IG FISMA metrics,[5] IGs 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 four (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.

Key Changes to the IG FISMA Reporting Metrics in FY 2024

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. In response to the threat environment and technology ecosystem which continue to evolve and change at a faster pace each year, OMB implemented a new framework regarding the timing and

[5] CIGIE, DHS, OMB, "FY 2023 – 2024 IG FISMA Reporting Metrics" https://www.cisa.gov/sites/default/files/2023-02/Final%20FY%202023%20-%202024%20IG%20FISMA%20Reporting%20Metrics%20v1.1_0.pdf.

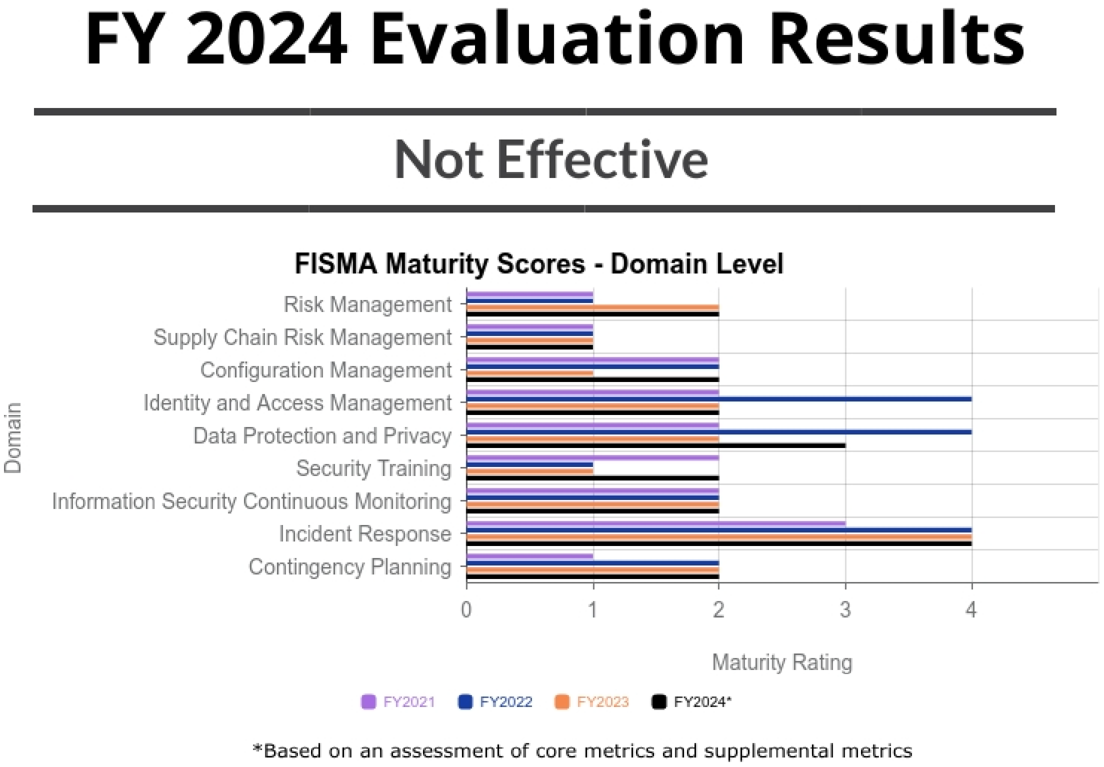
focus of assessments in FY 2022. The goal of this new framework was to provide agencies the opportunity to focus on the 20 most critical metrics, while establishing a triennial rotation of the remaining 46 supplemental metrics.

According to the IG FISMA metrics, one of the goals of the annual FISMA evaluation is to assess agency progress toward achieving outcomes that strengthen federal cybersecurity, including implementing the administration's priorities and best practices. The FY 2024 FISMA IG metrics focused on 20 core and 17 supplemental IG metrics and did not include the full suite of 66 metrics. The core IG Metrics were chosen based on alignment with Executive Order 14028, *Improving the Nation's Cybersecurity*, as well as recent OMB guidance to agencies. The supplemental IG metrics evaluated in 2024 were last evaluated in 2021.

Williams Adley utilized the criteria established by the federal government to evaluate the CPSC's FY 2024 information security program in accordance with FISMA. For a complete listing of criteria, please refer to Appendix A.3.

3. EVALUATION RESULTS

Based on the IG FISMA metric requirements, we concluded that the CPSC has made some improvements to its information security program and made progress in implementing some of the recommendations from previous FISMA evaluations, however, the CPSC has not implemented an effective information security program in FY 2024.



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

Figure 1. FY 2024 Evaluation 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 evaluation, Williams Adley identified deficiencies for each of the related IG FISMA metric domains. Each of the related conditions and supporting criteria are documented in the sections below.

Root Cause

The CPSC information security program was not effective because the CPSC still has not developed a comprehensive approach to manage 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. EXIT still has not received specific direction from senior management about how to integrate information security risk, including supply chain risks, into organization-wide risk management practices. Williams Adley has reported the lack of an ERM program since FY 2020. Moreover, EXIT, which is the office responsible for managing and implementing much of the CPSC's information security program and related practices, had a very high turnover in key positions in recent years and the CPSC reviewed open findings and recommendations based on workload. EXIT currently has two open positions and has prioritized remediation based on workload and available staff. We noted that the number of priorities competing for management's attention is increasing, and this trend does not appear to be waning. This amplifies the need for the CPSC to develop and leverage ERM to prioritize the remediation of information security deficiencies presented in this report.

Effect

The ineffective CPSC security program has led to data breaches in the past, and could again in the future lead to personally identifiable information, financial information, and other sensitive information becoming compromised. Due to the nature of the deficiencies identified, and the large amount of sensitive data handled by the CPSC, Williams Adley continues to be concerned with the strength of the existing information security program. 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 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 IG FISMA metric domains to create an effective information technology security program. Below we have provided a list of recommendations associated with each relevant condition. A majority of the recommendations

(32) identified below are directly related to prior year deficiencies and recommendations, while three (3) of the recommendations identified below are new this year as indicated by the parenthetical reference "(2024 recommendation)."

4.1 Identify Function Area

Progress

The CPSC has made progress in addressing previously identified Risk Management deficiencies in FY 2024. The CPSC has created policy and accompanying procedures for hardware and software asset management and software authorizations/approval.

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

Risk Management Conditions

Williams Adley determined that the CPSC was operating at **Maturity Level 2- Defined** for the Risk Management IG FISMA metric domain. Without effectively implementing a comprehensive risk management 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 information security risk management program in place the CPSC cannot ensure the information security efforts align with the CPSC's mission and organizational priorities.

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

i. The CPSC has not implemented the newly developed Information System Registration & Inventory Procedures.

ii. The CPSC has not fully defined system boundaries.

iii. The CPSC has not developed 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 (including the risk executive function) or equivalent
   - 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 risks
   - processes for communication of the risk management strategy across the CPSC
   - the technology utilized to support the CPSC's information security program
   - the development and use of a cybersecurity risk register or comparable mechanism

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

v. The CPSC has not defined 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.

vi. The CPSC has not fully developed an information security architecture or an enterprise architecture. The CPSC has also not defined its processes for ensuring that new or acquired hardware and software, including mobile apps, are consistent with its security architecture prior to introducing systems into its development environment.

vii. The CPSC does not utilize automation to perform scenario analysis and modeling of potential responses or leverage technology to guide the information security risk management program and to meet NIST requirements.

Supply Chain Risk Management Conditions

Williams Adley determined that the CPSC was operating at **Maturity Level 1 - Ad-hoc** for the SCRM IG FISMA metric domain. Without effectively implementing a comprehensive SCRM process at all levels of the organization, the CPSC may be unable to address the root causes associated with existing information security 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 SCRM IG FISMA metric domain:

i. The CPSC has not developed and formalized an organization-wide SCRM strategy/plan.

ii. The CPSC has not developed and formalized procedures and processes to ensure that CPSC-defined products, system components, systems, and services adhere to its cybersecurity and SCRM requirements. In addition, the CPSC has not defined and communicated its component authenticity procedures.

Identify Function Recommendations

We recommend that the CPSC:

1. Define and document the taxonomy of the CPSC's information system components, and classify each information system component as, at minimum, one of the following types: information technology system (e.g., proprietary and/or owned by the CPSC), application (e.g., commercial off-the-shelf, government off-the-shelf, or custom software), laptops and/or personal computers, service (e.g., external services that support the CPSC's operational mission, facility, or social media) (*Risk Management 2020 recommendation*).
2. Identify and implement a Network Access Control solution that establishes set policies for hardware and software access on the agency's network (*Risk Management 2020 recommendation*).
3. Develop and implement a formal strategy to address information security risk management requirements as prescribed by the NIST guidance (*Risk Management 2020 recommendation*).

4. 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 Management 2020 recommendation*).
5. Develop and implement an Enterprise Risk Management program based on NIST, Chief Financial Officers Council and Performance Improvement Council *Enterprise Risk Management Playbook*, and OMB Circular A-123, Section II guidance. This includes establishing a cross-departmental risk executive (function) led by senior management to provide both a departmental and organization level view of risk to the top decision makers within the CPSC (*Risk Management 2020 recommendation*).
6. Develop, document, and implement a process for determining and defining system boundaries in accordance with NIST guidance (*Risk Management 2021 recommendation*).
7. Develop and implement an information security architecture that supports the enterprise architecture (*Risk Management 2021 recommendation).*
8. Develop an enterprise architecture to be integrated into the risk management process (*Risk Management 2021 recommendation)*.
9. Implement solutions to perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting impact to organizational systems and data (*Risk Management 2022 recommendation*).
10. Implement registration and inventorying procedures for the CPSC's information systems (*Risk Management 2022 recommendation*).
11. Develop 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 (*SCRM 2021 recommendation – modified)*.
12. Develop and communicate an organization-wide Supply Chain Risk Management strategy/plan to manage the supply chain risks associated with the research, development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the CPSC systems, system components, or services (*SCRM 2023 recommendation*).

4.2 Protect Function Area

Progress

The CPSC has made progress on open prior year recommendations. The CPSC has developed a configuration management policy in accordance with the most recent NIST guidance. The CPSC has also developed various other policies and procedures that support configuration management. For example, the CPSC has developed server patching standard operating procedures and workstation patching standard operating procedures. Furthermore, the CPSC has also updated its vulnerability management policies and procedures, however the documents are in draft and going through management review and approval.

The CPSC has also made progress in addressing previously identified IAM 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 developed the policies and procedures for provisioning, managing, and reviewing privileged accounts.

In addition, the CPSC made progress in addressing previously identified DPP deficiencies. For example, the CPSC has developed a new data protection policy and media sanitization procedures. The documented procedures are currently undergoing final review and approval by CPSC management. The CPSC has also implemented security controls for data at rest, data in transit, and media protection. Furthermore, EXIT management stated that the CPSC is in the process of implementing data loss prevention policies.

Lastly, the CPSC has made progress in addressing previously identified Security Training deficiencies in FY 2024. The CPSC has finalized its Awareness and Training policy and drafted a Security and Privacy Training Plan. Furthermore, the CPSC has begun identifying personnel with significant security and/or privacy responsibilities in order to ensure that they receive role-based training moving forward.

Configuration Management Conditions

Williams Adley determined that the CPSC was operating at **Maturity Level 2 – Defined** for the configuration management IG FISMA metric domain. An effective configuration management program is critical to identify and mitigate vulnerabilities that can be exploited within the CPSC's environment. By not taking the strategic steps to develop and implement proper configuration plans and procedures, 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 configuration management IG FISMA metric domain:

i. The CPSC has not developed procedures to:
   a. ensure that configuration settings/common secure configurations are defined, implemented, and monitored
   b. document and manage deviations from authorized configuration settings/common secure configurations
ii. The CPSC has not established an Enterprise-wide Configuration Management Plan.
iii. The CPSC has not developed procedures to ensure that baseline configurations for its information systems are developed, documented, and maintained under configuration control. In addition, system components are not inventoried at a level of granularity necessary for tracking and reporting.
iv. The CPSC has policies related to the hardening of devices that are authorized for travel; however, the CPSC has not developed policies and procedures for the hardening of its other devices and information systems.

v. The CPSC does not monitor, analyze, and report qualitative and quantitative performance measures on the effectiveness of its change control activities.

vi. The CPSC has not established policies and procedures in support of Binding Operational Directive (BOD) 22-01, *Reducing the Significant Risk of Known Exploitable Vulnerabilities*, or consistently implemented its current policies and procedures addressing flaw remediation.

Identity and Access Management Conditions

Williams Adley determined that the CPSC was operating at **Maturity Level 2 – Defined** for the IAM IG FISMA metric domain. An effective IAM program is critical to prevent unauthorized system access. By not taking the strategic steps to develop and implement proper IAM procedures and authentication methods, the risk of unauthorized access to CPSC's systems is increased. Unauthorized access may result in improper access to and dissemination of confidential data, and other malicious activities.

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

i. The CPSC has not finalized Directives System Order 0311, *Policies and Procedures Governing the Personnel Security and Suitability Program*, of the CPSC that governs its processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its information systems.

ii. The CPSC has not fully implemented its processes for provisioning, managing, and reviewing privileged accounts.

Data Protection and Privacy Conditions

Williams Adley determined that the CPSC was operating at **Maturity Level 3- Consistently Implemented** for the DPP IG FISMA metric domain. An effective DPP program is critical to protect personally identifiable information and other sensitive data, as well as prevent data loss. By not taking the strategic steps to develop and implement proper procedures and training, the risk of unauthorized access to all forms of sensitive data is increased.

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

i. The CPSC has not fully implemented a data loss prevention tool.

ii. The CPSC has not developed role-based privacy awareness training for all applicable personnel. Specifically, while the CPSC has defined privacy training in the CPSC Privacy Program Plan, the CPSC has not defined requirements for role-based privacy awareness training and no role-based trainings have been provided to date.

Security Training Conditions

Williams Adley determined that the CPSC was operating at **Maturity Level 2 – Defined** for the Security Training IG FISMA metric domain. An effective security training program is critical to protecting the confidentiality, integrity, and availability of systems and data. Without understanding the information security knowledge, skills, and abilities required; or identifying the knowledge, skills, and abilities CPSC information security personnel are missing; the CPSC's training program may not be sufficient. Lack of adequate training may cause staff to unknowingly compromise the security of the CPSC's systems.

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

i. The CPSC has not developed or implemented a process for conducting information security personnel capability gap assessments, and the CPSC has not defined how frequently the assessment must be conducted and updated.
ii. The CPSC has not defined a process for measuring the effectiveness of its security awareness training.
iii. The CPSC has not formalized the Security and Privacy Training Plan which defines the following components:
    a. structure of the awareness and training program
    b. priorities
    c. funding
    d. goals of the program
    e. target audiences
    f. types of courses/material for each audience
    g. use of technologies (such as email advisories, intranet updates/wiki pages/social media, web-based training, phishing simulation tools)
    h. frequency of training
    i. deployment methods
iv. The CPSC has not defined its security training material based on its organizational requirements, culture, and the types of roles with significant security responsibilities.

Protect Function Recommendations

We recommend that the CPSC:

13. Develop, implement, and disseminate a set of configuration management procedures in accordance with the inherited configuration management policy which includes the process management follows to develop and tailor common secure configurations (hardening guides) and to approve deviations from those standard configurations (*Configuration Management 2020 recommendation*).
14. Integrate the management of secure configurations into the organizational configuration management process (*Configuration Management 2020 recommendation*).
15. Develop and implement an enterprise Configuration Management plan to ensure it includes all requisite information (*Configuration Management 2021 recommendation - modified*).
16. Develop and implement policies and procedures in support of Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities* (*Configuration Management 2022 recommendation*).
17. Develop qualitative and quantitative performance measures to evaluate the effectiveness of the following: Configuration Management plan and change control activities (*Configuration Management 2024 recommendation*).

18. Develop, formalize (through the CPSC's D-100 process), and implement processes to ensure all personnel are assigned risk designations and appropriately screened prior to being granted access to agency systems. Prior to formalizing the existing risk designation procedures, these procedures should be enhanced to include the following requirements:
    - Performance of periodic reviews of risk designations, at least annually,
    - Explicit position screening criteria for information security role appointments,
    - Description of how cybersecurity is integrated into human resources practices (*IAM 2020 recommendation*).
19. Implement the CPSC's policies and procedures for provisioning, managing, and reviewing privileged accounts (*IAM 2021 recommendation - modified*).
20. Identify all CPSC personnel that affect security and privacy (e.g., Executive Risk Council, Freedom of Information Act personnel, etc.) and ensure the training policies are modified to require these individuals to participate in role-based security/privacy training (*DPP 2020 recommendation*).
21. Fully implement a data loss prevention solution (*DPP 2020 recommendation - modified*).
22. Perform an assessment of the knowledge, skills, and abilities of CPSC personnel with significant security responsibilities (*Security Training 2020 recommendation*).
23. Develop and tailor security training content for all CPSC personnel with significant security responsibilities and provide this training to the appropriate individuals (*Security Training 2021 recommendation*).
24. Document and implement a process for ensuring that all personnel with significant security roles and responsibilities are provided specialized security training to perform assigned duties (*Security Training 2021 recommendation).*
25. Fully implement the Awareness and Training Policy (*Security Training 2023 recommendation - modified*).
26. Develop a security awareness and training strategy/plan in accordance with the Chief Human Capital Officers Council *Federal Cybersecurity Workforce Strategy* (*Security Training 2023 recommendation*).

4.3 Detect Function

Progress

The CPSC last authorized its major systems as of September 2023 and recently updated its System Assessment and Authorization policy. However, for FY 2024, the CPSC has not made progress in addressing previously identified ISCM deficiencies.

Information Security Continuous Monitoring Conditions

Williams Adley determined that the CPSC was operating at **Maturity Level 2 – Defined** for the ISCM IG FISMA metric domain. It is critical that organizations continuously monitor their systems to ensure implemented security controls remain effective. 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 or improve its security posture.

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

i. The ISCM Program is not designed in accordance with 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 *RMF for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Task P-7 (RMF Organization Level Prepare (P) Task), Continuous Monitoring Strategy – Organization, 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 *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, 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 consider business/mission impacts, however, no evidence could be provided to demonstrate this was done.

ii. 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 were based on a NIST security control catalog that is out-of-date. CPSC policies require minor applications are required to be assessed every three (3) years.

iii. The CPSC has not captured the information necessary to report on the qualitative and quantitative performance measures defined in the ISCM plan.

Detect Function Recommendations

We recommend that the CPSC:

27. 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 (*ISCM 2020 recommendation - modified*).
28. Implement Information Security Continuous Monitoring procedures including those procedures related to the monitoring of performance measures and metrics, that support the Information Security Continuous Monitoring program (*ISCM 2021 recommendation*).
29. Update the System Security Plans to include the most up-to-date information and assess the relevant minor applications (*ISCM 2022 recommendation).*

4.4 Respond Function

Progress

In FY 2024, the CPSC made progress in addressing previously identified Incident Response deficiencies. For example, the CPSC has started to procure additional tool sets and licenses in order to fulfill OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents,* compliance requirements.

Incident Response Conditions

Williams Adley determined that the CPSC was operating at **Maturity Level 4 – Managed and Measurable** for the Incident Response IG FISMA metric domain. Williams Adley noted that this is the third consecutive year that the CPSC's Incident Response program has been effective. An effective Incident Response program is critical for detecting, identifying, containing, eradicating, and recovering from security incidents. By not implementing the latest guidance it may decrease CPSC's ability to minimize the impact of an attack, remediate vulnerabilities, and secure its information systems. Furthermore, without defined, implemented, and mature Event Logging (EL) capabilities, the CPSC's ability to ensure visibility into the security posture of the agency is diminished. Williams Adley noted that the CPSC has not yet met the logging requirements to reach the EL 1 (basic) maturity level as defined in OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*. While EXIT is currently working on a project to enhance their logging capabilities to EL 2 (intermediate) by the end of FY 2024, OMB requires agencies to achieve EL 3 (advanced).

Respond Function Recommendations

We recommend that the CPSC:

30. Define and implement Event Logging requirements in accordance with OMB M 21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (*Incident Response 2023 recommendation*).

4.5 Recover Function

Progress

In FY 2024, the CPSC took a step towards addressing previously identified Contingency Planning deficiencies. The CPSC has formalized the new Contingency Planning policy to comply with the latest NIST guidance. Furthermore, the CPSC conducted Information System Contingency Plan testing for its major information systems.

Contingency Planning Conditions

Williams Adley determined that the CPSC was operating at **Maturity Level 2 – Defined** for the Contingency Planning 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 Contingency Planning program is critical for the recovery of the CPSC's operations in the event of a disaster or an outage. An outdated and incomplete Contingency Planning program increases the possibility of disruption and confusion, as well as limiting the CPSC's opportunity to return to normal operations safely in the shortest time possible.

Williams Adley identified the following deficiencies within the Contingency Planning 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:

   a. the system-level BIAs and Information System Contingency Plans 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.
   b. 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.
   c. 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 and this is an important factor when defining recovery priorities and tasks.
   d. 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 system contingency plans.
iv. The CPSC does not fully implement back up processes for General Support System Cloud.

Recover Function Recommendations

We recommend that the CPSC:

31. Update the Continuity of Operations Plan, or other documentation supporting CPSC 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 CPSC's continuity of operations (*Contingency Planning 2020 recommendation - modified*).
32. Integrate documented contingency plans with the newly developed Continuity of Operations Plan and organizational Business Impact Analyses *(Contingency Planning 2020 recommendation - modified*).
33. 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., NIST SP 800-34/53, DHS *Federal Continuity Directive 1*, NIST Cybersecurity Framework, and National Archives and Records Administration guidance) (*Contingency Planning 2023 recommendation*).
34. 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*).
35. Fully implement its processes for information system back up for General Support System Cloud (*Contingency Planning 2024 recommendation*).

5. Consolidated List of Recommendations

Table 5-1: Index of Recommendations

Finding	Recommendation
Identify (Risk Management)	1. Define and document the taxonomy of the CPSC's information system components, and classify each information system component as, at minimum, one of the following types: information technology system (e.g., proprietary and/or owned by the CPSC), application (e.g., commercial off-the-shelf, government off-the-shelf, or custom software), laptops and/or personal computers, service (e.g., external services that support the CPSC's operational mission, facility, or social media) (*Risk Management 2020 recommendation*). 2. Identify and implement a Network Access Control solution that establishes set policies for hardware and software access on the agency's network (*Risk Management 2020 recommendation*). 3. Develop and implement a formal strategy to address information security risk management requirements as prescribed by the NIST guidance (*Risk Management 2020 recommendation*). 4. 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 Management 2020 recommendation*). 5. Develop and implement an Enterprise Risk Management program based on NIST, Chief Financial Officers Council and Performance Improvement Council *Enterprise Risk Management Playbook*, and OMB Circular A-123, Section II guidance. This includes establishing a cross-departmental risk executive (function) led by senior management to provide both a departmental and organization level view of risk to the top decision makers within the CPSC (*Risk Management 2020 recommendation*). 6. Develop, document, and implement a process for determining and defining system boundaries in accordance with NIST guidance (*Risk Management 2021 recommendation*). 7. Develop and implement an information security architecture that supports the enterprise architecture (*Risk Management 2021 recommendation).* 8. Develop an enterprise architecture to be integrated into the risk management process (*Risk Management 2021 recommendation).* 9. Implement solutions to perform scenario analysis and model potential responses, including modeling the potential impact of a

	threat exploiting a vulnerability and the resulting impact to organizational systems and data (*Risk Management 2022 recommendation*). 10. Implement registration and inventorying procedures for the CPSC's information systems (*Risk Management 2022 recommendation*).
Identify (Supply Chain Risk Management)	11. Develop 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 (*SCRM 2021 recommendation – modified).* 12. Develop and communicate an organization-wide Supply Chain Risk Management strategy/plan to manage the supply chain risks associated with the research, development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the CPSC systems, system components, or services (*SCRM 2023 recommendation*).
Protect (Configuration Management)	13. Develop, implement, and disseminate a set of configuration management procedures in accordance with the inherited configuration management policy which includes the process management follows to develop and tailor common secure configurations (hardening guides) and to approve deviations from those standard configurations (*Configuration Management 2020 recommendation*). 14. Integrate the management of secure configurations into the organizational configuration management process (*Configuration Management 2020 recommendation*). 15. Develop and implement an enterprise Configuration Management plan to ensure it includes all requisite information (*Configuration Management 2021 recommendation - modified*). 16. Develop and implement policies and procedures in support of Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities* (*Configuration Management 2022 recommendation*). 17. Develop qualitative and quantitative performance measures to evaluate the effectiveness of the following: Configuration Management plan and change control activities (*Configuration Management 2024 recommendation*).
Protect (Identity and Access Management)	18. Develop, formalize (through the CPSC's D-100 process), and implement processes to ensure all personnel are assigned risk designations and appropriately screened prior to being granted access to agency systems. Prior to formalizing the existing risk designation procedures, these procedures should be enhanced to include the following requirements: • Performance of periodic reviews of risk designations, at least annually,

	- Explicit position screening criteria for information security role appointments, - Description of how cybersecurity is integrated into human resources practices (*IAM 2020 recommendation*). 19. Implement the CPSC’s policies and procedures for provisioning, managing, and reviewing privileged accounts (*IAM 2021 recommendation - modified*).
Protect (Data Protection and Privacy)	20. Identify all CPSC personnel that affect security and privacy (e.g., Executive Risk Council, Freedom of Information Act personnel, etc.) and ensure the training policies are modified to require these individuals to participate in role-based security/privacy training (*DPP 2020 recommendation*). 21. Fully implement a data loss prevention solution (*DPP 2020 recommendation - modified*).
Protect (Security Training)	22. Perform an assessment of the knowledge, skills, and abilities of CPSC personnel with significant security responsibilities (*Security Training 2020 recommendation*). 23. Develop and tailor security training content for all CPSC personnel with significant security responsibilities and provide this training to the appropriate individuals (*Security Training 2021 recommendation*). 24. Document and implement a process for ensuring that all personnel with significant security roles and responsibilities are provided specialized security training to perform assigned duties (*Security Training 2021 recommendation).* 25. Fully implement the Awareness and Training Policy (*Security Training 2023 recommendation - modified*). 26. Develop a security awareness and training strategy/plan in accordance with the Chief Human Capital Officers Council *Federal Cybersecurity Workforce Strategy* (*Security Training 2023 recommendation*).
Detect (Information Security Continuous Monitoring)	27. 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 (*ISCM 2020 Recommendation - modified*). 28. Implement Information Security Continuous Monitoring procedures including those procedures related to the monitoring of performance measures and metrics, that support the Information Security Continuous Monitoring program (*ISCM 2021 recommendation*).

	29. Update the System Security Plans to include the most up-to-date information and assess the relevant minor applications (*ISCM 2022 recommendation).*
Respond (Incident Response)	30. Define and implement Event Logging requirements in accordance with OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (*Incident Response 2023 recommendation*).
Recover (Contingency Planning)	31. Update the Continuity of Operations Plan, or other documentation supporting CPSC 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 CPSC's continuity of operations (*Contingency Planning 2020 recommendation - modified*). 32. Integrate documented contingency plans with the newly developed Continuity of Operations Plan and organizational Business Impact Analyses *(Contingency Planning 2020 recommendation - modified*). 33. 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., NIST SP 800-34/53, DHS *Federal Continuity Directive 1*, NIST Cybersecurity Framework, and National Archives and Records Administration guidance) (*Contingency Planning 2023 recommendation*). 34. 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*). 35. Fully implement its processes for information system back up for General Support System Cloud (*Contingency Planning 2024 recommendation*).

Appendix A: Objective, Scope and Methodology

A.1 Objective

The objective was to perform an independent evaluation of the CPSC's implementation of FISMA[6] for FY 2024. In support of this objective, Williams Adley conducted the evaluation in accordance with OMB M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*.

A.2 Scope

The evaluation focused on reviewing the CPSC's implementation of FISMA for FY 2024 based on OMB M-24-04. The FISMA evaluation covered the period of July 1, 2023, to June 30, 2024. The evaluation included an assessment of 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 evaluation included an assessment of the NIST Cybersecurity Framework Function Levels, as specified in the FY 2024 IG FISMA reporting core metrics:

- Identify (Risk Management)
- Identify (Supply Chain Risk 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 2024 IG FISMA Reporting Metrics developed by the OMB, DHS, and CIGIE are intended to provide guidance on the OIG annual evaluations, as required by FISMA, 44 U.S.C. 3555(j).

We performed this evaluation from March through July 2024 and conducted this evaluation in accordance with CIGIE *Quality Standards for Inspection and Evaluation*. Those standards require that we obtain sufficient evidence to provide a reasonable basis for our findings and conclusions

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

based on our evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our review objectives.

To perform this evaluation, we interviewed CPSC senior management and employees to evaluate 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. We delivered the Notices of Findings and Recommendations for each IG FISMA function to CPSC management.

Use of Computer-Processed Data

During the evaluation, 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 within FY 2024 for testing. The list was used to support the evaluation 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 evaluation. 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 evaluation, 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 evaluation, 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*.[7] 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 not exist in other information systems that were not tested.

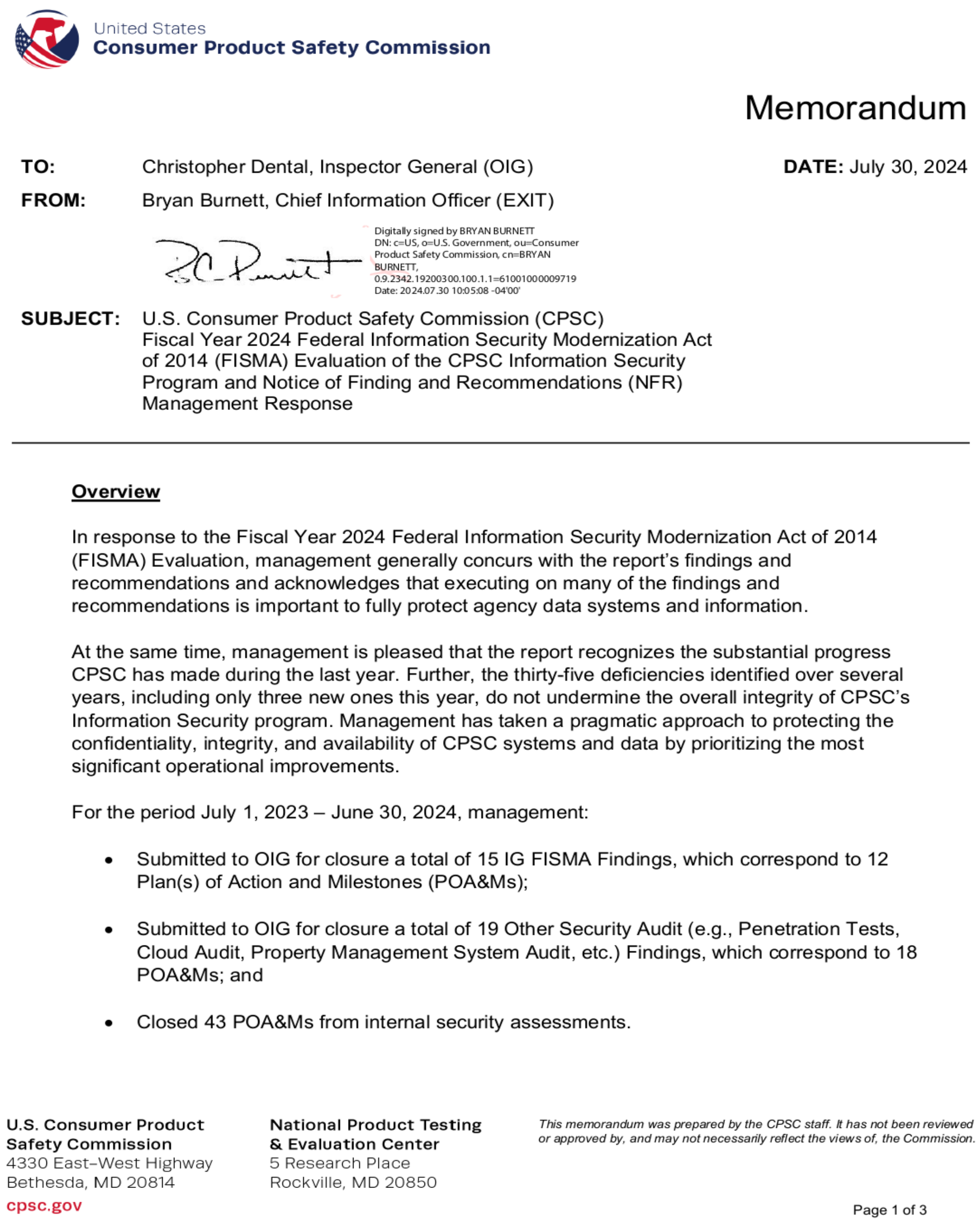
[7] American Institute of Certified Public Accountants *Audit Guide*, *Audit Sampling*, March 1, 2014.

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

- Center for Internet Security Top 18 Security Controls
- Chief Information Officer Council/Chief Acquisition Officer Council, *Cloud Computing Contract Best Practices*
- Cybersecurity and Infrastructure Security Agency (CISA), *Capacity Enhancement Guide*
- CISA, *Cybersecurity & Incident Response Playbooks*
- CISA, *Zero Trust Maturity Model*
- DHS BOD 18-02
- DHS BOD 19-02
- DHS BOD 22-01
- DHS BOD 23-01
- DHS Cyber Incident Reporting: Unified Message
- DHS Emergency Directive 19-01
- DHS Information and Communications Technology Supply Chain Library
- Executive Order 13636
- Executive Order 13800
- Executive Order 13870
- Executive Order 14028
- Federal Acquisition Supply Chain Security Act of 2018
- Federal Continuity Directive 1
- Federal Continuity Directive 2
- Federal Cybersecurity Workforce Assessment Act of 2015
- Federal Enterprise Architecture Framework v.2
- Federal Information Processing Standards 199
- Federal Information Processing Standards 201-2
- FISMA
- Federal Information Technology Acquisition Reform Act
- Federal Risk and Authorization Management Program - Standard Contract Clauses
- Fiscal Year 2022 and 2023 Chief Information Officer Federal Information Security Modernization Act Metrics
- Fiscal Year 2022 Senior Agency Official for Privacy FISMA
- General Accountability Office, *Standards for Internal Control in the Federal Government*
- Homeland Security Presidential Directive 12
- National Cybersecurity Workforce Framework
- National Insider Threat Policy
- NIST Cybersecurity Framework
- NIST Interagency Report 8011
- NIST Interagency Report 8170
- NIST Interagency Report 8179
- NIST Interagency Report 8276
- NIST Interagency Report 8286
- NIST Interagency Report 8374
- NIST Interagency Report 8397
- NIST SP 800-18

- NIST SP 800-34
- NIST SP 800-37, Rev. 2
- NIST SP 800-39
- NIST SP 800-40, Rev. 4
- NIST SP 800-50
- NIST SP 800-53, Rev. 5
- NIST SP 800-60
- NIST SP 800-61, Rev. 2
- NIST SP 800-63
- NIST SP 800-70, Rev. 4
- NIST SP 800-83
- NIST SP 800-122
- NIST SP 800-128
- NIST SP 800-137
- NIST SP 800-152
- NIST SP 800-157
- NIST SP 800-160
- NIST SP 800-161, Rev. 1
- NIST SP 800-163, Rev. 1
- NIST SP 800-181
- NIST SP 800-207
- NIST SP 800-209
- NIST SP 800-218
- NIST SP 1800-5
- OMB Circular A-123
- OMB Circular A-130
- OMB M 14-03
- OMB M 15-14
- OMB M 16-17
- OMB M 19-03
- OMB M 19-17
- OMB M 20-04
- OMB M 21-07
- OMB M 21-30
- OMB M 21-31
- OMB M 22-01
- OMB M 22-09
- OMB M 22-18
- OMB M 23-03
- Presidential Policy Directive 8: National Preparedness
- Presidential Policy Directive-41
- Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act
- Title 5, Code of Federal Regulations
- US-Computer Emergency Readiness Team, *Incident Notification Guidelines*

Appendix B: Management Responses



United States
Consumer Product Safety Commission

Memorandum

TO: Christopher Dental, Inspector General (OIG)

DATE: July 30, 2024

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: 2024.07.30 10:05:08 -04'00'

SUBJECT: U.S. Consumer Product Safety Commission (CPSC) Fiscal Year 2024 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 2024 Federal Information Security Modernization Act of 2014 (FISMA) Evaluation, management generally concurs with the report's findings and recommendations and acknowledges that executing on many of the findings and recommendations is important to fully protect agency data systems and information.

At the same time, management is pleased that the report recognizes the substantial progress CPSC has made during the last year. Further, the thirty-five deficiencies identified over several years, including only three new ones this year, do not undermine the overall integrity of CPSC's Information Security program. Management has taken a pragmatic approach to protecting the confidentiality, integrity, and availability of CPSC systems and data by prioritizing the most significant operational improvements.

For the period July 1, 2023 – June 30, 2024, management:

- Submitted to OIG for closure a total of 15 IG FISMA Findings, which correspond to 12 Plan(s) of Action and Milestones (POA&Ms);

- Submitted to OIG for closure a total of 19 Other Security Audit (e.g., Penetration Tests, Cloud Audit, Property Management System Audit, etc.) Findings, which correspond to 18 POA&Ms; and

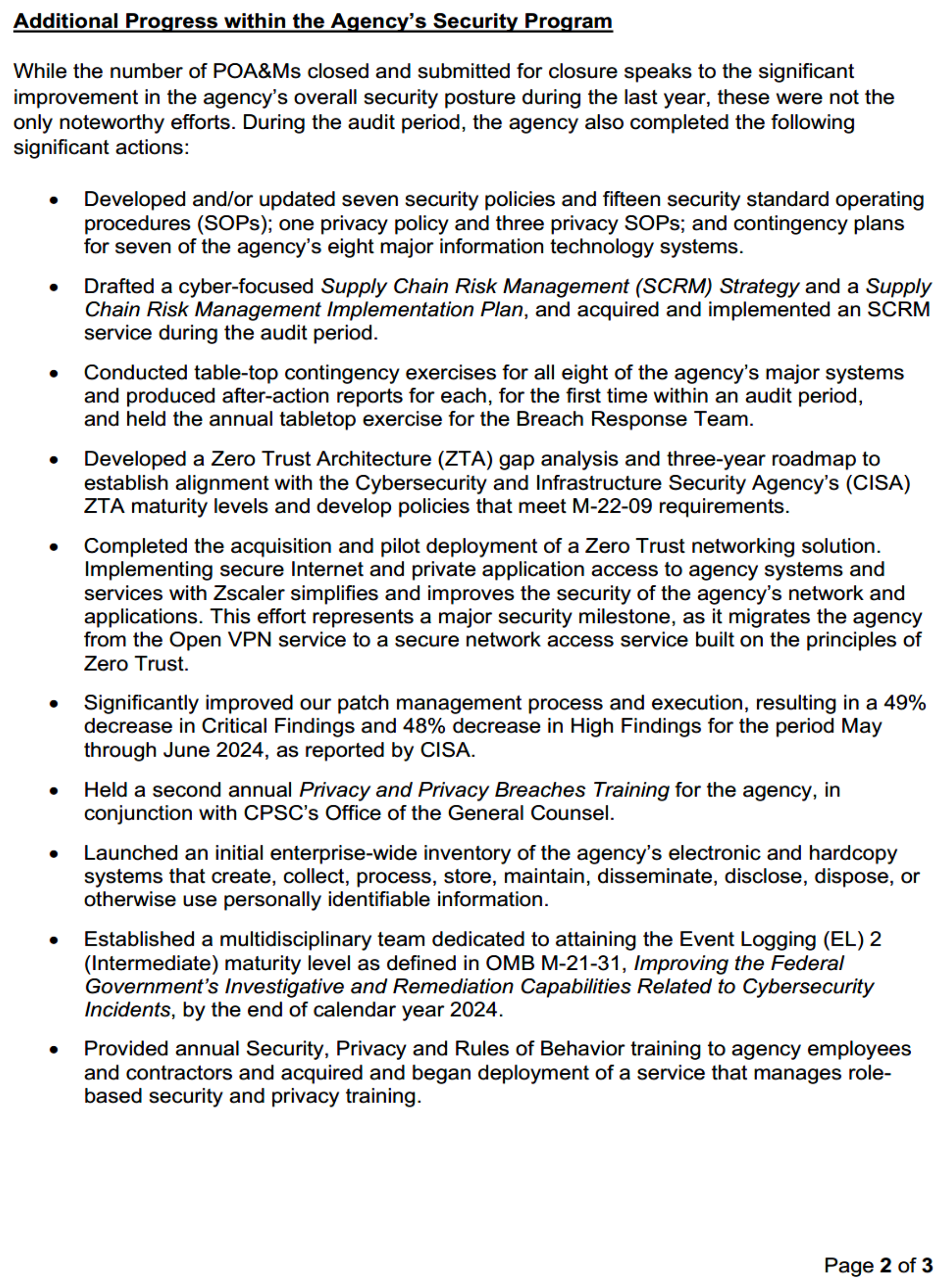
- Closed 43 POA&Ms from internal security assessments.

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.

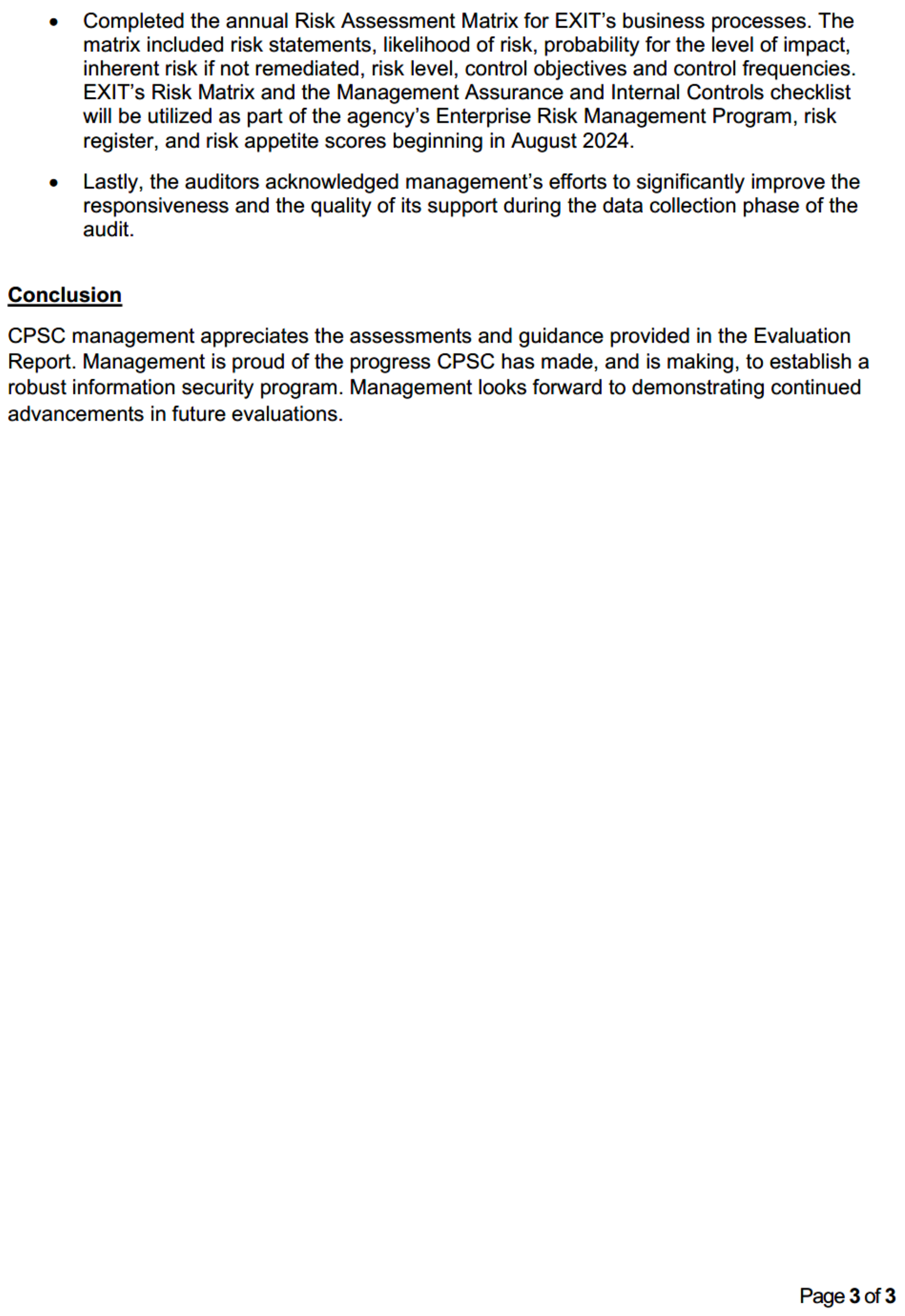
Page 1 of 3



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:

- Developed and/or updated seven security policies and fifteen security standard operating procedures (SOPs); one privacy policy and three privacy SOPs; and contingency plans for seven of the agency's eight major information technology systems.
- Drafted a cyber-focused *Supply Chain Risk Management (SCRM) Strategy* and a *Supply Chain Risk Management Implementation Plan*, and acquired and implemented an SCRM service during the audit period.
- Conducted table-top contingency exercises for all eight of the agency's major systems and produced after-action reports for each, for the first time within an audit period, and held the annual tabletop exercise for the Breach Response Team.
- Developed a Zero Trust Architecture (ZTA) gap analysis and three-year roadmap to establish alignment with the Cybersecurity and Infrastructure Security Agency's (CISA) ZTA maturity levels and develop policies that meet M-22-09 requirements.
- Completed the acquisition and pilot deployment of a Zero Trust networking solution. Implementing secure Internet and private application access to agency systems and services with Zscaler simplifies and improves the security of the agency's network and applications. This effort represents a major security milestone, as it migrates the agency from the Open VPN service to a secure network access service built on the principles of Zero Trust.
- Significantly improved our patch management process and execution, resulting in a 49% decrease in Critical Findings and 48% decrease in High Findings for the period May through June 2024, as reported by CISA.
- Held a second annual *Privacy and Privacy Breaches Training* for the agency, in conjunction with CPSC's Office of the General Counsel.
- Launched an initial enterprise-wide inventory of the agency's electronic and hardcopy systems that create, collect, process, store, maintain, disseminate, disclose, dispose, or otherwise use personally identifiable information.
- Established a multidisciplinary team dedicated to attaining the Event Logging (EL) 2 (Intermediate) maturity level as defined in OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, by the end of calendar year 2024.
- Provided annual Security, Privacy and Rules of Behavior training to agency employees and contractors and acquired and began deployment of a service that manages role-based security and privacy training.



- Completed the annual Risk Assessment Matrix for EXIT's business processes. The matrix included risk statements, likelihood of risk, probability for the level of impact, inherent risk if not remediated, risk level, control objectives and control frequencies. EXIT's Risk Matrix and the Management Assurance and Internal Controls checklist will be utilized as part of the agency's Enterprise Risk Management Program, risk register, and risk appetite scores beginning in August 2024.
- Lastly, the auditors acknowledged management's efforts to significantly improve the responsiveness and the quality of its support during the data collection phase of the audit.

Conclusion

CPSC management appreciates the assessments and guidance provided in the Evaluation Report. Management is proud of the progress CPSC has made, and is making, to establish a robust information security program. Management looks forward to demonstrating continued advancements in future evaluations.

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