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

Evaluation of the CPSC's FISMA Implementation for FY 2023

July 28, 2023

23-A-05

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 28, 2023

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

FROM: Christopher W. Dentel, Inspector General

Christopher W. Dentel
Digitally signed by Christopher W. Dentel
Date: 2023.07.31 10:28:37 -04'00'

SUBJECT: Evaluation of the CPSC's FISMA Implementation for FY 2023

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 2023, 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 Quality Standards for Inspection and Evaluation (QSIE). We reviewed the resulting report and related documentation and made relevant inquires 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.

In conducting their evaluation, 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. 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 44 recommendations. The CPSC closed two of the prior years' recommendations and thirteen new recommendations were made. Should you have any questions about this report, please contact me.

Table of Contents

Abbreviations and Short Titles 2
EXECUTIVE SUMMARY 3
WHAT WE FOUND 3
WHAT WE RECOMMEND 4
1. OBJECTIVE 5
2. BACKGROUND AND CRITERIA 5
3. EVALUATION RESULTS 11
4. FINDING: The CPSC Has Not Implemented an Effective Information Security Program 12
5. Consolidated List of Recommendations 27
Appendix A: Objective, Scope and Methodolog 32
A.1 Objective 32
A.2 Scope 32
A.3 Methodology 32
Appendix B: Management Responses 36

Abbreviations and Short Titles

BIA	Business Impact Analysis
BOD	Binding Operational Directive
CIGIE	Council of Inspectors General on Integrity and Efficiency
CISA	Cybersecurity and Infrastructure Security Agency
COOP	Continuity of Operations Plan
CPSC	U.S. Consumer Product Safety Commission
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
ICAM	Identity, Credential, and Access Management (ICAM)
IG	Inspector General
ISCM	Information Security Continuous Monitoring
M	Memorandum
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
POA&M	Plans of Actions and Milestones
Rev.	Revision
SCRM	Supply Chain Risk Management
SOP	Standard Operating Procedure
SP	Special Publication
TIC	Trusted Internet Connection
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 Inspectors General for Integrity and Efficiency (CIGIE) limited the scope of the evaluation to 20 "core" and 20 supplemental reporting metrics in fiscal year (FY) 2023.

The U.S. Consumer Product Safety Commission (CPSC) OIG retained Williams, Adley, & Co.-DC LLP (Williams Adley), an independent public accounting firm, to perform the independent evaluation of the CPSC's implementation of FISMA for FY 2023 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 1, "ad hoc," to level five, "optimized," with level 4, "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 two recommendations through the continued implementation of its privileged user access management solution. This implementation has allowed the CPSC to enforce Personal Identification Verification card authentication for and adequately restrict access to privileged accounts. The CPSC also made progress on remediating several other FISMA recommendations, specifically:

- The CPSC maintained its ongoing authorization for its major systems and tracked system-level Information Security Continuous Monitoring (ISCM) performance measures and metrics.
- The CPSC updated its awareness and training policy.
- The CPSC defined its Supply Chain Risk Management (SCRM) policy.
- The CPSC developed a Continuity of Operation Plan (COOP) which includes a business process analysis and business impact assessment (BIA) for each of CPSC identified Mission Essential Functions.
- The CPSC has encrypted all of its databases, virtual machines, and workstations.

- The CPSC implemented an effective mechanism to support the timely reports of its security incidents to the Cybersecurity Infrastructure Security Agency (CISA).

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 adequately prioritize addressing the information security weaknesses identified in the OIG's previous FISMA evaluations. Turnover of effectively all the key personnel responsible for the governance of the CPSC's information security program which included the Chief Information Officer, the Chief Information Security Officer, and the Director of Information Technology and Technical Services, delayed progress in addressing recommendations in FY 2023. This in combination with the lack of an enterprise risk management program and guidance from CPSC senior leadership on how to integrate information security risk management continues to hinder the further development of the information security program. Another challenge facing the CPSC that has prevented the closure of prior year recommendations is the CPSC's continued failure to implement an effective Enterprise Risk Management (ERM) program which provides direction and guidance to those responsible for the information security program. An effective ERM 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 44 recommendations that the CPSC must address in order to mature its information security program. We provided 14 new recommendations and reissued 30 prior year 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 2023.

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)-23-03, *Fiscal Year 2023 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 44 deficiencies across 9 domains. Key deficiencies included a lack of an effective risk management processes and an effective contingency planning program which resulted from the CPSC not taking a holistic approach to manage information security risks and utilize information security resources to address previously identified information security deficiencies.

We made 44 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 (30) carried over from previous years; however, we made 14 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 (NIST) Risk Management Framework

NIST established the information security risk management best practices via the risk management framework as detailed in the NIST Special Publication (SP) 800-37, Revision (Rev.) 2, *Risk Management Framework for Information Systems and Organizations*, and NIST SP 800-39, *Managing Information Security Risk*. The NIST Risk Management Framework 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 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:

---

[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.

- **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 Cybersecurity Framework. Understanding the business context, the resources that support critical functions, and the related information security risks enables 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. The protect function supports the ability to limit or contain the impact of a potential cybersecurity event.
- **Detect –** The detect function requires the development and implementation of appropriate activities to identify the occurrence of a cybersecurity event. The detect function enables timely discovery of a cybersecurity event.
- **Respond –** The respond function requires the development and implementation of appropriate activities to take regarding a detected cybersecurity event. The respond function supports the ability to 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 restore any capabilities or services that were impaired because of a cybersecurity event. The recover function supports timely return to normal operations to reduce the impact from an information security 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 2023 IG FISMA Reporting Metrics identified 20 core metrics and 20 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 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 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, credential, 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 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 data protection and privacy performance measures.

3. **Detect Function**

- *Information Security Continuous Monitoring* – An agency with an effective information security continuous monitoring program maintains ongoing authorizations of information systems; integrates metrics on the effectiveness of its information security continuous monitoring 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 information security continuous monitoring 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 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.

[5] CIGIE, DHS, OMB, "FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (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

Key Changes to the IG FISMA Reporting Metrics in FY 2023

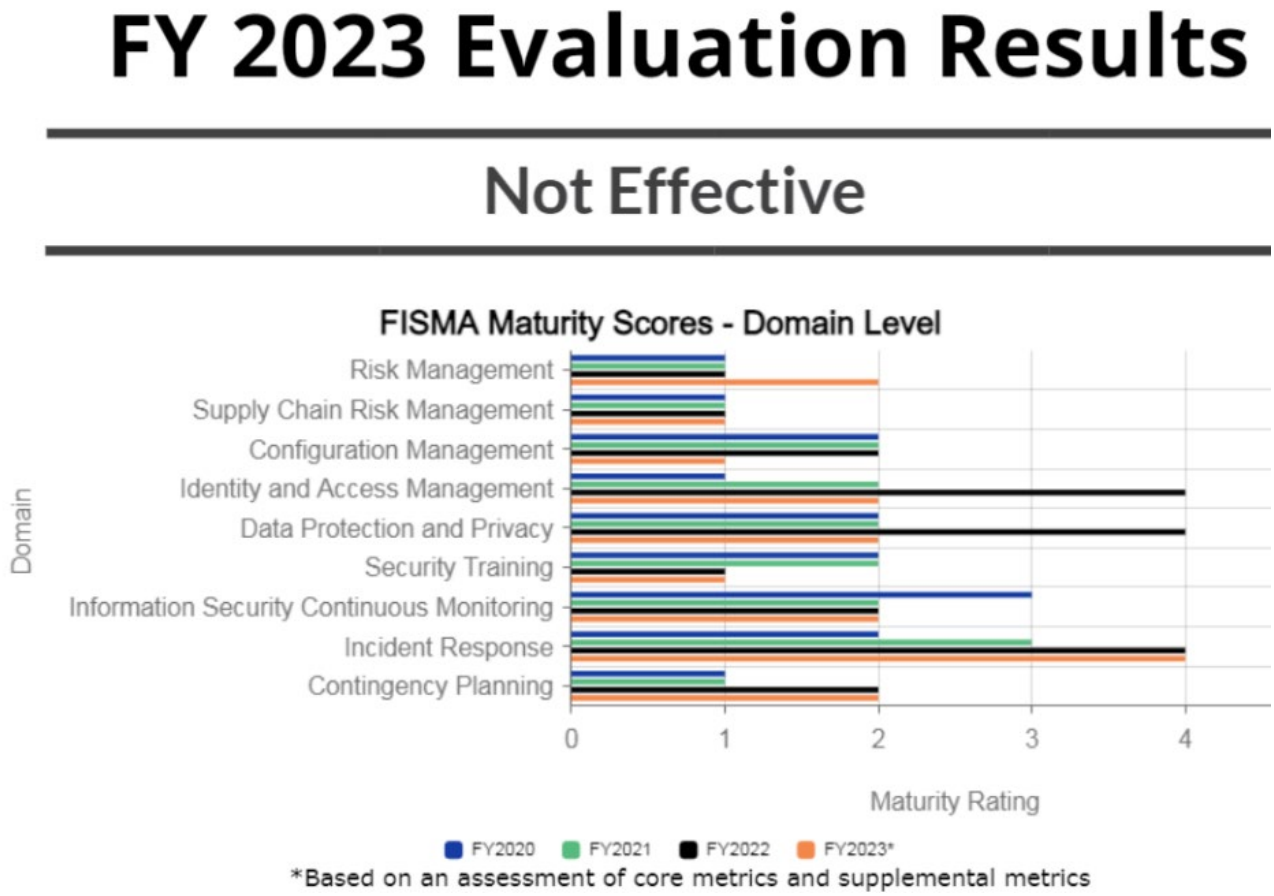
Reflecting OMB's shift in emphasis away from compliance in favor of risk management, IGs are encouraged to evaluate the IG metrics based on the risk tolerance and threat model of their agency and to focus on the practical security impact of weak control implementations, rather than strictly evaluating 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 focus of assessments in FY2022. The goal of this new framework was to provide a more flexible but continued focus on annual assessments for the federal community.

According to the IG FISMA metrics, one of the goals of the annual FISMA evaluation is to assess agencies' progress toward achieving outcomes that strengthen federal cybersecurity, including implementing the administration's priorities and best practices. The FY 2023 FISMA IG metrics focused on 20 core and 20 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.

Williams Adley utilized the criteria established by the federal government to evaluate the CPSC's FY 2023 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 although the CPSC has made some improvements to its information security program and made progress in implementing some of the recommendations from previous FISMA evaluations, the CPSC has not implemented an effective information security program in FY 2023.



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

Figure 3-1. FY 2023 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 holistic formal 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 insufficient, and the Office of Information and Technology Services (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, the office responsible for managing and implementing much of the CPSC's information security program and related practices, had very high turnover in key positions during the past year which appeared to delay the remediation of previously identified deficiencies.

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

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. Data breaches at the CPSC have in the past, and could again in the future, lead to personally identifiable information (PII), financial information, and other sensitive information becoming compromised. 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.

Further, without an effective information security program, the CPSC mission to keep consumers safe will remain at risk. 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.

Recommendations

The CPSC must address the individual conditions presented in the IG FISMA metric domains. Below we have provided a list of recommendations associated with each relevant condition. A majority of the recommendations (30) identified below are directly related to prior year deficiencies and recommendations, while 14 of the recommendations identified below are new this year as indicated by the parenthetical reference "(2023 recommendation)."

4.1 Identify Function Area

Progress

The CPSC has not made progress in addressing previously identified Risk Management deficiencies in FY 2023.

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, and we identified 75 applications that were not known, authorized, and tracked by management.

Information System Inventory

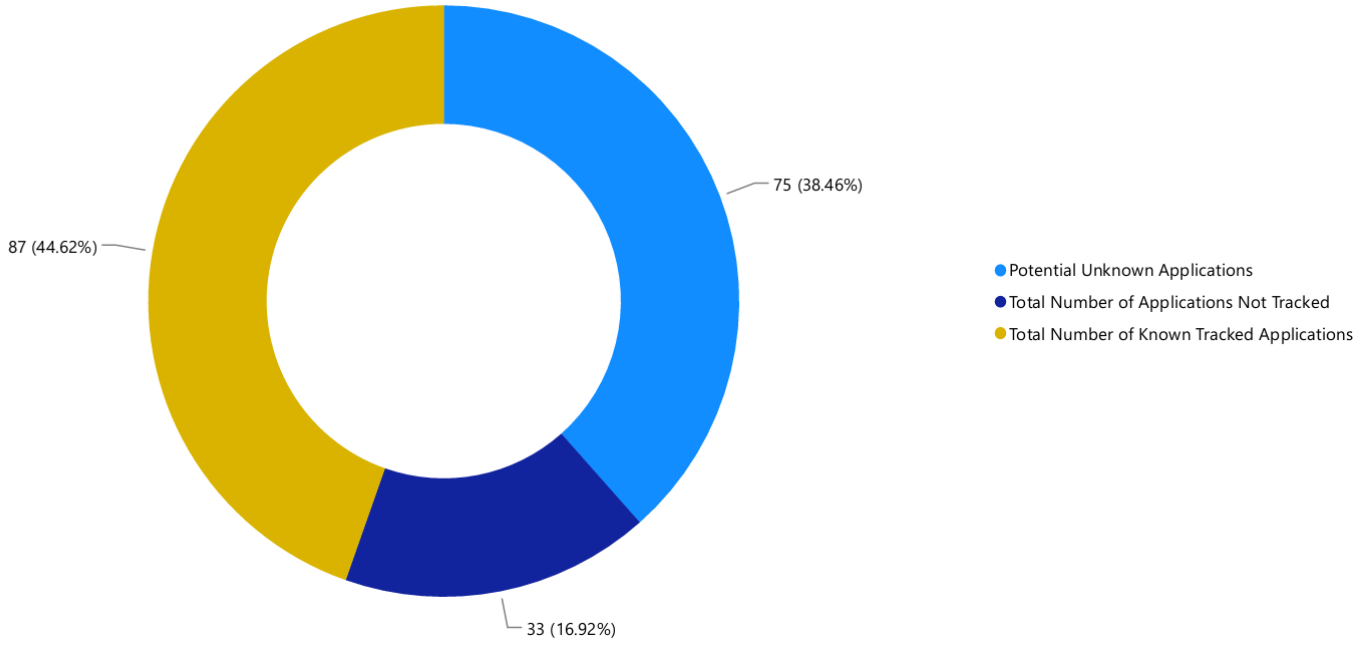
Williams Adley completed additional evaluation procedures to highlight the importance of establishing a complete and accurate information system inventory. Specifically, Williams Adley surveyed the CPSC program offices in an effort to identify specific deficiencies in the official information system inventory provided and to gain better insight into the systems in use at the CPSC. As part of this survey, department heads were asked to provide a list of all applications, software tools, third-party/cloud services, etc. their departments used and to indicate which they deemed "essential" to operations.

The CPSC department leadership's responses provided us with a number of items that were not included in the official information system inventory provided by EXIT as did our review of the applications available on the agency's intranet. We noted that these discrepancies could be a result of a lack of coordination between the CPSC departments and because CPSC management has not established procedures that adequately defined what the CPSC considers to be an

"information system" or how CPSC management determines the boundary of an information system.

A visualization of our analysis results is presented in the figure below. Overall, we identified a total of 195 applications, 87 of which were tracked in the CPSC's system inventory, 33 of which were listed on the CPSC's intranet but not included in the systems inventory, and 75 of which were not listed on the CPSC's intranet or tracked in the CPSC's system inventory, therefore, potentially unknown to EXIT.

Figure 4-1. Information System Inventory Analysis



Additional risk management conditions include:

i. The CPSC has not fully defined system boundaries.
ii. The CPSC has not developed a process for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting.
iii. The CPSC has not developed a process for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses utilized in the organization's environment with the detailed information necessary for tracking and reporting.
iv. 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, 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

v. 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.

vi. 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.

vii. The CPSC has not consistently implemented Plans of Actions and Milestones (POA&M) in accordance with agency procedure to mitigate security weaknesses, for example certain POA&Ms are significantly overdue, and the POA&Ms did not include an estimate of the funding necessary or the source of that funding.

viii. The CPSC has not performed periodic lessons learned to improve the POA&M processes.

ix. 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

The CPSC has made progress in addressing the SCRM deficiencies previously identified. For example, the CPSC started to conduct a supply chain risk assessment, however, all of the SCRM documents provided remain in draft form. Therefore, 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 supply chain risk management 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 externally sourced products, system components, systems, and services.

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

i. The CPSC has not defined and communicated policies, 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.

ii. The CPSC has not defined and communicated an organization wide SCRM strategy/plan.

Identify Function Recommendations

1. Implement registration and inventorying procedures for the CPSC's information systems (*Risk Management 2022 Recommendation*).
2. Develop, document, and implement a process for determining and defining system boundaries in accordance with National Institute of Standards and Technology guidance (*Risk Management 2021 Recommendation*).
3. Establish and implement a policy and procedures to manage software licenses using automated monitoring and expiration notifications (*Risk Management 2020 Recommendation*).
4. Establish and implement a policy and procedures to ensure that only authorized hardware and software execute on the agency's network (*Risk Management 2020 Recommendation).*
5. 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*).
6. 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*).
7. Develop and implement a formal strategy to address information security risk management requirements as prescribed by the National Institute of Standards and Technology guidance (*Risk Management 2020 Recommendation*).
8. 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*).
9. Develop and implement an Enterprise Risk Management program based on National Institute of Standards and Technology, Enterprise Risk Management Playbook, and Office of Management and Budget 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*).
10. Implement Plan of Action and Milestones in accordance with agency policy to mitigate security weakness and document the estimated funding requirements for each of the Plan of Action and Milestones along with the source of those funds (*Risk Management 2023 Recommendation*).
11. Perform periodic lessons learned exercises to improve the Plan of Action and Milestones process (*Risk Management 2023 Recommendation*).

12. 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*).
13. 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 (*Supply Chain Risk Management 2021 Recommendation – modified*).
14. 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 (*Supply Chain Risk 2023 Recommendation*).

4.2 Protect Function Area

Progress

The CPSC has made progress in addressing the previously identified Configuration Management deficiencies in FY 2023. For example, the CPSC is currently developing a Zero Trust Policy which will cover all Trusted Internet Connection (TIC) version 3.0 requirements and many other requirements outlined in the Zero Trust pillars. In addition, the CPSC made progress on other open prior year recommendations but not enough to close any of them.

The CPSC has also made progress in addressing previously identified Identity and Access Management deficiencies in FY 2022. For example, the CPSC has developed a Standard of Operating Procedures (SOP) for the management of privileged user accounts and formalized this SOP just prior to conclusion of field work.

Furthermore, the CPSC made progress in addressing previously identified Data Protection and Privacy (DPP) deficiencies in FY 2023. Every CPSC database, virtual machine, and workstation is encrypted. The CPSC also utilizes an automated tool to detect removable devices on CPSC workstations.

Lastly, the CPSC has made progress in addressing previously identified Security Training deficiencies in FY 2023. For example, the CPSC has updated its Awareness and Training Policy. However, this policy had not been signed by CPSC management before the end of our fieldwork.

Configuration Management Conditions

Williams Adley determined that the CPSC was operating at Maturity Level 1 – Ad-Hoc 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's configuration management policies are out-of-date and do not align with the current NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Rev. 5. Also, 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 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.
iii. The CPSC has not established procedures for documenting, managing, and monitoring deviations from agreed upon configuration settings.
iv. The CPSC has not established policies and procedures in support of Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploitable Vulnerabilities*, or consistently implemented its current policies and procedures addressing flaw remediation.
v. The CPSC has not prepared and planned to meet the goals of the TIC initiative, consistent with OMB M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative*. Specifically, the agency has not defined and customized, as appropriate, its policies, procedures, and processes to implement TIC 3.0. These should include updating the CPSC's network and system boundary policies, in accordance with OMB M-19-26. These processes also include, as appropriate, meeting the requirements in the TIC security capabilities catalog, defining specific TIC use cases, and designing/documenting TIC overlays. Moreover, the CPSC has not defined processes to develop and maintain an accurate inventory of its network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection.
vi. The CPSC has not updated its Vulnerability Disclosure Handling Procedures to support the implementation of its Vulnerability Disclosure Program.

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. Although the CPSC scored Level 2 – Defined, Williams Adley identified deficiencies that impact the overall information security program effectiveness. 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. The CPSC has made progress in addressing previously identified IAM deficiencies in FY 2022. For example, the CPSC has developed a SOP for the management of privileged user accounts and formalized this SOP just prior to conclusion of field work.

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

i. The CPSC's Identity and Access Management policies are out-of-date and do not align with the current NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Rev. 5.
ii. The CPSC has not developed an Identity, Credential, and Access Management (ICAM) strategy.
iii. The CPSC has not defined the following procedures for their ICAM program:
    - account management processes for both privileged and non-privileged users
    - separation of duties and use of least privilege
    - identification and authentication procedures
iv. The CPSC has not implemented a process to review its current ICAM practices, identify gaps in its ICAM strategy and processes, and develop an ICAM transition plan to guide the CPSC from its current state to its desired state.
v. The CPSC has not defined its processes for developing and maintaining user access agreements.
vi. The CPSC has not fully implemented its processes for provisioning, managing, and reviewing privileged accounts.
vii. The CPSC does not log and actively monitor privileged user activity or the activity of those who have incompatible duties.
viii. The CPSC was unable to provide evidence of the existence of procedures which define remote access configuration/connection requirements, including use of Federal Information Processing Standards 140-2 validated cryptographic modules, system timeouts, and monitoring and control of remote access sessions.

Data Protection and Privacy Conditions

Williams Adley determined that the CPSC was operating at Maturity Level 2- Defined for the DPP IG FISMA metric domain. An effective DPP program is critical to protect PII and prevent data loss. The CPSC made progress in addressing previously identified DPP deficiencies in FY 2023. Every CPSC database, virtual machine, and workstation is encrypted. The CPSC also utilizes an automated tool to detect removable devices on CPSC workstations. By not taking the strategic

steps to develop and implement proper procedures and training, the risk of unauthorized access to PII and other sensitive data is increased. In addition, without a complete understanding of the types and locations of PII and other types of sensitive data within CPSC's environment, the CPSC may not be able to appropriately mitigate the risk of a data breach.

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

i. The CPSC has not developed a process for maintaining and tracking PII inventory (the types of PII records maintained by system and their sources).
ii. The CPSC has not fully implemented its encryption of data at rest and encryption of data in transit policies.
iii. CPSC has not conducted a data exfiltration tabletop exercise.

Security Training Conditions

Williams Adley determined that the CPSC was operating at Maturity Level 1 – Ad-hoc for the Security Training IG FISMA metric domain. The CPSC has made progress in addressing previously identified Security Training deficiencies in FY 2023. For example, the CPSC has updated its Awareness and Training Policy. However, this policy had not been signed by CPSC management before the end of our fieldwork. 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 of the knowledge, skills, and abilities CPSC information security personnel are missing, the CPSC's training program may not be sufficient. By not taking the strategic steps necessary to develop and implement tailored training that will provide those needed skills, personnel may unsuspectingly compromise the security of the CPSC's systems.

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

i. Management was unable to provide evidence that the roles and responsibilities outlined in the agency awareness and training policy were implemented.
ii. The CPSC has not consistently implemented its security awareness and training policy. Specifically, 4 out of 10 users sampled did not complete their security training within five (5) days of their entry on duty date.
iii. 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.
iv. The CPSC has not developed a security training plan or strategy 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

Protect Function Recommendations

We recommend that the CPSC:

15. Develop, implement, and disseminate a current configuration management policy which is in accordance with the most recent National Institute of Standards and Technology guidance (*Configuration Management 2023 Recommendation*).
16. 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*).
17. Integrate the management of secure configurations into the organizational configuration management process *(Configuration Management 2020 Recommendation)*.
18. Develop, implement, and disseminate processes to implement Trusted Internet Connection 3.0, including updating its network and system boundary policies, in accordance with Office of Management and Budget Memorandum 19-26, *Update to the Trusted Internet Connections (TIC) Initiative*. This includes, as appropriate, the incorporation of TIC security capabilities catalog, TIC use cases, and TIC overlays (*Configuration Management 2023 Recommendation*).
19. Develop and implement policies and procedures in support of Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploitable Vulnerabilities* (*Configuration Management 2022 Recommendation).*
20. Update the Vulnerability Disclosure Handling Procedures to support the implementation of the CPSC's Vulnerability Disclosure Program (*Configuration Management 2023 Recommendation*).
21. Develop, implement, and disseminate an Identity and Access Management policy and procedures which are in accordance with the most recent National Institute of Standards and Technology guidance (*Identity and Access Management 2023 Recommendation)*.
22. Define and document a strategy (including specific milestones) to implement the Federal Identity, Credential, and Access Management architecture (*Identity and Access Management 2020 Recommendation)*.
23. Integrate Identity, Credential, and Access Management strategy and activities into the Enterprise Architecture and Information Security Continuous Monitoring (*Identity and Access Management 2020 Recommendation)*.
24. Define and implement the Identity, Credential, and Access Management policies and procedures (*Identity and Access Management 2020 Recommendation)*.
25. Define and implement a process to ensure the completion of access agreements for all CPSC users (*Identity and Access Management 2020 Recommendation)*.

26. Implement the CPSC's policies and procedures for provisioning, managing, and reviewing privileged accounts (*Identity and Access Management 2021 Recommendation - modified).*
27. Identify and document potentially incompatible duties permitted by privileged accounts (*Identity and Access Management 2020 Recommendation)*.
28. Log and actively monitor activities performed while using privileged access that permit potentially incompatible duties (*Identity and Access Management 2020 Recommendation).*
29. Define and document policies and procedures outlining the CPSC's remote access configuration/connection requirements, including use of Federal Information Processing Standards 140-2 validated cryptographic modules, system timeouts, and monitoring and control of remote access sessions (*Identity and Access Management 2023 Recommendation)*.
30. Implement data encryption policies and procedures for data at rest and data in transit. This should include fully implementing the Data Loss Prevention solution (*Data Protection & Privacy 2020 Recommendation - Modified*).
31. Document and implement a process for inventorying and securing systems that contain Personally Identifiable Information or other sensitive agency data (e.g., proprietary information) (*Data Protection & Privacy 2020 recommendation*).
32. Document and implement a process for periodically reviewing for and removing unnecessary Personally Identifiable Information from agency systems (*Data Protection & Privacy 2020 Recommendation*).
33. Perform an assessment of the knowledge, skills, and abilities of the CPSC personnel with significant security responsibilities (*Security Training 2020 Recommendation*).
34. Finalize and implement the Awareness and Training policy which is currently in draft (*Security Training 2023 Recommendation*).
35. Develop a security awareness and training strategy/plan in accordance with Federal Cybersecurity Workforce Strategy (*Security Training 2023 Recommendation*).

4.3 Detect Function

Progress

The CPSC has authorized its major systems and tracks system-level ISCM performance measures and metrics. However, the CPSC has not made any 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 *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, 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 *Information Security Continuous Monitoring (ISCM) 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 NIST security control catalog that is out-of-date. In addition, CPSC policies require minor applications to be assessed every three (3) years.
iii. The CPSC has not consistently implemented assigned ISCM roles and responsibilities to ensure that all required tasks are being carried out. For example, NIST SP 800-137, section 3.1 requires each tier to monitor security metrics and assess security control effectiveness with established monitoring and assessment frequencies and status reports customized to support tier-specific decision making. However, no evidence could be provided to show this was done and the CPSC has not explicitly established any mechanisms to enforce accountability for those with ISCM responsibilities.

Detect Function Recommendations

We recommend that the CPSC:

36. 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*).
37. Update the System Security Plans to include the most up-to-date information and assess the relevant minor applications (*ISCM 2022 Recommendation).*
38. Implement Information Security Continuous Monitoring roles and responsibilities (*ISCM 2023 Recommendation).*
39. Develop mechanisms to ensure Information Security Continuous Monitoring stakeholder accountability (*ISCM 2023 Recommendation).*

4.4 Respond Function

Progress

In FY 2023, the CPSC made progress in addressing previously identified Incident Response deficiencies. For example, CPSC has established network profiling techniques and implemented an effective process to detect and analyze incidents. In addition, the CPSC has implemented effective mechanisms to support the timely reporting of its security incidents to CISA United States (US)-Computer Emergency Readiness Team. The CPSC has also implemented explicit performance measures to evaluate the effectiveness of its incident response capabilities and program. Furthermore, the CPSC completed a procurement of additional network monitoring licenses for Event Logging (EL) purposes, with the expectation that these licenses will allow the CPSC to reach EL3 (advanced). The CPSC is in the process of hiring two additional candidates to perform vulnerability management and cloud security tasks which will free up existing resources to support compliance with the event logging requirements outlined in OMB M 21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents.*

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. However, Williams Adley noted that the CPSC has not yet met the logging requirements required to reach the EL1 (basic) maturity level, and OMB requires agencies to achieve EL 1 (basic), EL2 (intermediate) and EL3 (advanced).

Respond Function Recommendations

We recommend that the CPSC:

40. Define and implement event logging requirements in accordance with Office of Management and Budget Memorandum 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 2023, the CPSC took the initial step towards addressing previously identified Contingency Planning deficiencies. For example, the CPSC has developed a COOP which includes a business process analysis and BIA for each of the CPSC identified Mission Essential Functions. Additionally, the CPSC began drafting a new Contingency Planning policy to comply with the latest guidance and to replace the current Contingency Planning policy which was last updated in 2019.

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 and data availability is essential to an organization's success; therefore, it is critical that the CPSC's information systems operate effectively and do so without excessive interruption. An effective contingency planning program is critical for the recovery of CPSC operations in the event of a disaster or an outage. By not integrating contingency planning into the other relevant CPSC planning areas, it increases the possibility of disruption and confusion, as well as limits the CPSC's opportunity to return to normal operations in the safest and shortest time possible.

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

i. The CPSC has not developed policies and procedures for all its contingency planning processes including, but not limited to, conducting organizational and system level BIAs and maintaining the agency COOP in addition the current contingency planning policies and procedures are based on an out-of-date guidance.
ii. The CPSC did not include all necessary information into its COOP or integrated its COOP and organizational-level BIAs with its system-level BIAs or its Information System Contingency Plans. 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.
iii. System level BIAs are out-of-date.
iv. The CPSC has not provided evidence to support information system contingency planning testing and recovery activities for four (4) out of seven (7) major systems.

Recover Function Recommendations

We recommend that the CPSC:

41. 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, Federal Continuity Directive 1, National

Institute of Standards and Technology Cybersecurity Framework, and National Archive and Records Administration guidance) (*Contingency Planning 2023 Recommendation*).

42. Update the Continuity of Operations Plan, or other documentation supporting the 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*).
43. Integrate documented contingency plans with the newly developed Continuity of Operations Plan and organizational Business Impact Analyses (*Contingency Planning 2020 Recommendation - modified*).
44. Test the set of documented contingency plans (*Contingency Planning 2020 Recommendation).*

5. Consolidated List of Recommendations

Table 5-1: Index of Recommendations

Finding	Recommendation
Identify (Risk Management)	1. Implement registration and inventorying procedures for the CPSC's information systems (*Risk Management 2022 Recommendation*). 2. Develop, document, and implement a process for determining and defining system boundaries in accordance with National Institute of Standards and Technology guidance (*Risk Management 2021 Recommendation*). 3. Establish and implement a policy and procedures to manage software licenses using automated monitoring and expiration notifications (*Risk Management 2020 Recommendation*). 4. Establish and implement a policy and procedure to ensure that only authorized hardware and software execute on the agency's network (*Risk Management 2020 Recommendation).* 5. 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*). 6. 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*). 7. Develop and implement a formal strategy to address information security risk management requirements as prescribed by the National Institute of Standards and Technology guidance (*Risk Management 2020 Recommendation*). 8. 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*).

	9. Develop and implement an Enterprise Risk Management program based on National Institute of Standards and Technology, Enterprise Risk Management Playbook, and Office of Management and Budget 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*). 10. Implement Plan of Action and Milestones in accordance with agency policy to mitigate security weakness and document the estimated funding requirements for each of the Plan of Action and Milestones along with the source of those funds (*Risk Management 2023 Recommendation*). 11. Perform periodic lessons learned exercises to improve the Plan of Action and Milestones process (*Risk Management 2023 Recommendation*). 12. 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*).
Identify (Supply Chain Risk Management)	13. 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 (*Supply Chain Risk Management 2021 Recommendation – modified*). 14. 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 (*Supply Chain Risk 2023 Recommendation*).
Protect (Configuration Management)	15. Develop, implement, and disseminate a current configuration management policy which is in accordance with the most recent National Institute of Standards and Technology guidance (*Configuration Management 2023 Recommendation*). 16. 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*). 17. Integrate the management of secure configurations into the organizational configuration management process *(Configuration Management 2020 Recommendation)*. 18. Develop, implement, and disseminate processes to implement Trusted Internet Connection 3.0, including updating its network and system boundary policies, in accordance with Office of Management and Budget Memorandum 19-26, *Update to the Trusted Internet Connections (TIC) Initiative*. This includes, as appropriate, the incorporation of Trusted Internet Connection security capabilities catalog, Trusted Internet Connection use cases, and Trusted Internet Connection overlays (*Configuration Management 2023 Recommendation*). 19. Develop and implement policies and procedures in support of Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploitable Vulnerabilities* (*Configuration Management 2022 Recommendation)*. 20. Update the Vulnerability Disclosure Handling Procedures to support the implementation of the CPSC's Vulnerability Disclosure Program (*Configuration Management 2023 Recommendation*).
Protect (Identity and Access Management)	21. Develop, implement, and disseminate an Identity and Access Management policy and procedures which are in accordance with the most recent National Institute of Standards and Technology guidance (*Identity and Access Management 2023 Recommendation)*. 22. Define and document a strategy (including specific milestones) to implement the Federal Identity, Credential, and Access Management architecture (*Identity and Access Management 2020 Recommendation)*. 23. Integrate Identity, Credential, and Access Management strategy and activities into the Enterprise Architecture and Information Security Continuous Monitoring (*Identity and Access Management 2020 Recommendation)*. 24. Define and implement the Identity, Credential, and Access Management policies and procedures (*Identity and Access Management 2020 Recommendation)*. 25. Define and implement a process to ensure the completion of access agreements for all of the CPSC users (*Identity and Access Management 2020 Recommendation)*.

	26. Implement the CPSC's policies and procedures for provisioning, managing, and reviewing privileged accounts. (*Identity and Access Management 2021 Recommendation - modified).* 27. Identify and document potentially incompatible duties permitted by privileged accounts (*Identity and Access Management 2020 Recommendation).* 28. Log and actively monitor activities performed while using privileged access that permit potentially incompatible duties (*Identity and Access Management 2020 Recommendation).* 29. Define and document policies and procedures outlining the CPSC's remote access configuration/connection requirements, including use of Federal Information Processing Standards 140-2 validated cryptographic modules, system timeouts, and monitoring and control of remote access sessions (*Identity and Access Management 2023 Recommendation).*
Protect (Data Protection and Privacy)	30. Implement data encryption policies and procedures for data at rest and data in transit. This should include fully implementing the Data Loss Prevention solution (*Data Protection & Privacy 2020 Recommendation - Modified*). 31. Document and implement a process for inventorying and securing systems that contain Personally Identifiable Information or other sensitive agency data (e.g., proprietary information) (*Data Protection & Privacy 2020 recommendation*). 32. Document and implement a process for periodically reviewing for and removing unnecessary Personally Identifiable Information from agency systems (*Data Protection & Privacy 2020 Recommendation*).
Protect (Security Training)	33. Perform an assessment of the knowledge, skills, and abilities of the CPSC personnel with significant security responsibilities (*Security Training 2020 Recommendation*). 34. Finalize and implement the Awareness and Training policy which is currently in draft (*Security Training 2023 Recommendation*). 35. Develop a security awareness and training strategy/plan in accordance with Federal Cybersecurity Workforce Strategy (*Security Training 2023 Recommendation).*
Detect (Information Security Continuous Monitoring)	36. 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).* 37. Update the System Security Plans to include the most up-to-date information and assess the relevant minor applications (*ISCM 2022 Recommendation*). 38. Implement Information Security Continuous Monitoring roles and responsibilities (*ISCM 2023 Recommendation).* 39. Develop mechanisms to ensure Information Security Continuous Monitoring stakeholder accountability (*ISCM 2023 Recommendation).*
Respond (Incident Response)	40. Define and implement event logging requirements in accordance with Office of Management and Budget Memorandum 21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (*Incident Response 2023 Recommendation*).
Recover (Contingency Planning)	41. 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, Federal Continuity Directive 1, National Institute of Standards and Technology Cybersecurity Framework, and National Archive and Records Administration guidance) (*Contingency Planning 2023 Recommendation*). 42. Update the Continuity of Operations Plan, or other documentation supporting the 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*). 43. Integrate documented contingency plans with the newly developed Continuity of Operations Plan and organizational Business Impact Analyses (*Contingency Planning 2020 Recommendation - modified*). 44. Test the set of documented contingency plans (*Contingency Planning 2020 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 2023. In support of this objective, Williams Adley conducted the evaluation in accordance with OMB M-23-03, *Fiscal Year 2023 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 2023 based on OMB M-23-03. The FISMA evaluation covered the period of July 1, 2022, to June 30, 2023. 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 2023 IG FISMA reporting core metrics:

- Identify (Risk Management)
- Identify (Supply Chain Risk Management)
- Protect (Configuration Management)
- Protect (Identity and Access Management)
- Protect (Date 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 2023 IG FISMA Reporting Metrics developed by the OMB, DHS, and CIGIE are intended to provide guidance on the OIG's annual evaluations, as required by FISMA, 44 U.S.C. 3555(j).

We performed this evaluation from March through June 2023 and conducted this evaluation in accordance with CIGIE Quality Standards for Inspection and Evaluation. Those standards require

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

that we obtain sufficient evidence to provide a reasonable basis for our findings and conclusions 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 Williams Adley's 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 2023 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 Financial Officer Council, *Enterprise Risk Management for the U.S. Federal Government*
- Chief Information Officer Council/Chief Acquisition Officer Council, *Cloud Computing Contract Best Practices*
- CISA, *Cybersecurity & Incident Response Playbooks*
- CISA, *Cybersecurity Incident and Vulnerability Response Playbooks*
- Cybersecurity and Infrastructure Security Agency, *Zero Trust Maturity Model*
- DHS Binding Operational Directive (BOD) 18-02
- DHS BOD 19-02
- DHS BOD 22-01
- DHS BOD 19-01
- DHS BOD 23-01
- Executive Order 13636
- Executive Order 14028
- Federal Acquisition Supply Chain Security Act of 2018
- Federal Continuity Directive 1
- Federal Cybersecurity Workforce Assessment Act of 2015
- Federal Enterprise Architecture Framework v.2
- Federal Information Processing Standards 140-2
- Federal Information Processing Standards 199
- Federal Information Processing Standards 201-2
- Federal Risk and Authorization Management Program - Standard Contract Clauses
- *Fiscal Year 2023 Chief Information Officer Federal Information Security Modernization Act Metrics*
- Homeland Security Presidential Directive 12
- National Cybersecurity Workforce Framework
- NIST Cybersecurity Framework
- NIST Interagency Report 8011
- NIST Interagency Report 8276
- NIST Interagency Report 8286
- NIST SP 800-18
- NIST SP 800-34
- NIST SP 800-37, Rev. 2
- NIST SP 800-39
- NIST SP 800-40, Rev. 3
- NIST SP 800-50
- NIST SP 800-53, Rev. 5
- NIST SP 800-61, Rev. 2
- NIST SP 800-63
- NIST SP 800-128

- NIST SP 800-70, Rev. 4
- NIST SP 800-137
- NIST SP 800-152
- NIST SP 800-157
- NIST SP 800-181
- NIST SP 800-207
- NIST SP 800-218
- NIST SP 1800-5
- OMB Circular A-123
- OMB Circular A-130
- OMB M 14-03
- 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 23-03
- OMB M 21-31
- OMB M 22-01
- OMB M 22-05
- OMB M 22-09
- OMB M 23-03
- US-Computer Emergency Readiness Team, *Incident Response Guidelines*

Appendix B: Management Responses

United States
Consumer Product Safety Commission

Memorandum

TO: Office of Inspector General **DATE:** July 28, 2023

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: 2023.07.28 09:28:38 -04'00'

SUBJECT: U.S. Consumer Product Safety Commission (CPSC) Fiscal Year 2023 Federal Information Security Modernization Act of 2014 (FISMA) Evaluation of the CPSC Information Security Program and Notice of Finding and Recommendations (NFR) Management Response

---

Management concurs with the included findings and recommendations and offers the following context and updates by domain.

Identify (Risk Management)

EXIT presently is updating its inventory of minor applications, linking them to the appropriate General Support System (GSS) or major application, and assessing them, as required. This response also is applicable to the NFR for *Detect (Information Security Continuous Monitoring)*.

EXIT recently procured a solution to manage software licenses and their expirations. We expect to complete deploying and configuring this automated toolset in fiscal year 2024.

EXIT presently is drafting a policy and accompanying procedures for hardware and software asset management and software authorizations/approvals. The estimated completion date is in fiscal year 2024.

EXIT recently completed the implementation of wired network access control (NAC) for agency laptops. We continue to work on controlled wireless access and expanding the scope to include agency mobile devices.

EXIT presently is reviewing all prior risk acceptance approvals, assessing these risks based on the methodology/processes established in NIST 800-37/30. The estimated completion date is in fiscal year 2024

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 4

One of the early efforts led by the new Chief Information Security Officer (CISO) was to begin developing a consolidated list of existing Plan of Actions and Milestones (POA&Ms) and establishing a tracking mechanism with estimated completion dates. EXIT is working to update its standard operating procedure (SOP) to reflect this, and other, significant process improvements. EXIT estimates the completion date for finalizing the list and processes is in fiscal year 2024.

The agency already owns a variety of tools to model potential responses to and the impact of a threat exploiting a vulnerability. Within the past few months, EXIT detected multiple incidents and leveraged its cybersecurity tools to examine the extent and impact of each. EXIT will demonstrate to the Office of Inspector General (OIG) how it leveraged its tools and procedures to respond to these incidents.

Identify (Supply Chain Risk Management)

EXIT is at the midpoint of developing an effective Supply Chain Risk Management (SCRM) program. A SCRM policy was authored last year and, presently, an SCRM Assessment SOP is being reviewed by management. EXIT continues to conduct market research for SCRM services, meeting with multiple vendors and research services in recent weeks. Once a selection is made for vendor assessment services, the SOP will be finalized and integrated within the EXIT's System Development Life Cycle (SDLC). Hardware and software purchases then will be reviewed and assessed prior to award and annually, thereafter.

Protect (Configuration Management)

EXIT is in the process of updating its Configuration Management (CM) policy. The policy will align with NIST 800-53 CM controls and will be used to guide the implementation of configuration management within the organization. EXIT expects to finalize the policy in fiscal year 2024.

EXIT understands that the development/implementation of applicable Trusted Internet Connectivity (TIC) use cases and overlays requires procuring services that meet TIC 3.0 requirements. EXIT recently acquired secure Internet and private access services, which will serve as the foundational components of a comprehensive network redesign. This strategic effort will not only enhance our network's security and reliability but also play a crucial role in defining how users authenticate at the application and network layers, as well as how access should be provisioned. The project kickoff is planned for August 2023.

An updated Vulnerability Management Policy is currently in management review. After it is finalized, EXIT will develop an accompanying SOP that covers the different types of vulnerability alerts and reports. EXIT expects to finalize its Vulnerability Management Policy and SOP in fiscal year 2024.

EXIT plans to migrate to the Vulnerability Disclosure Policy (VDP) Platform provided by CISA. The migration has been put on hold until we are able backfill a vacant Vulnerability Management position.

Protect (Identity and Access Management)

As is noted in the report, EXIT has made progress in the management of privileged user accounts, from both policy and technical perspectives. More recently, we have extended the management of privileged accounts into our productivity software as a service (SaaS) and, by the end of the calendar year, will have done the same for our other cloud services. EXIT's Event Logging program presently logs and reviews privileged user activity and will be enhanced as the program matures.

The agency's multiple modernization efforts – including for case management, data collection and manipulation, and data analytics – all provide significant improvements in the supported authentication and authorization methods over the systems they are replacing. While our current policies will need to span both legacy and modern systems, these new methods will improve the agency's identity and access management postures significantly.

EXIT has begun developing a new Identity, Credential, and Access Management (ICAM) policy and the accompanying procedures. These are significant efforts that require a holistic review of the agency's ICAM program. As such, we expect the policy and procedures to be completed and in place in fiscal year 2024.

Protect (Data Protection and Privacy)

EXIT presently is developing an inventory process for Personally Identifiable Information (PII). We expect the resultant inventory to completed in fiscal year 2024. EXIT also is developing an SOP for periodically reviewing and removing unnecessary PII from agency systems. These procedures are expected to be finalized and will be promulgated to agency program offices in fiscal year 2024.

Protect (Security Training)

EXIT recently updated its security and privacy training policy to address annual security training, annual privacy training, and role-based security training. Once the new policy is signed and its contents are communicated, EXIT plans to enforce compliance.

EXIT recently procured a SaaS training platform to manage its role-based security training program. After an initial gap assessment, EXIT expects to implement its role-based security training plan and system in fiscal year 2024.

Respond (Incident Response)

As noted in the report, EXIT presently is backfilling its Vulnerability Management position, which will assist the security team in focusing on Event Logging (EL). Additionally, EXIT recently completed the procurement of additional network monitoring licenses and services for EL purposes. Onboarding of the contractors and initial implementation of the new licenses is set to begin in September 2023.

Recover (Contingency Planning)

The agency enacted an updated Continuity of Operations (COOP) plan on January 26, 2023. The development of the updated COOP plan included enterprise business process and impact assessments. EXIT will utilize the plan and the accompanying assessments to guide maturation of its contingency planning/disaster recovery program, including:

- Updating its Contingency Planning Policy. As noted in the report, a draft currently is in review.
- Applying a consistent approach, with templates, to its annual contingency planning and disaster recovery exercises for all major systems.
- Requiring system owners to maintain the results of contingency planning and disaster recovery exercises in the Cyber Security Assessment and Management (CSAM) application, as part of the agency's Assessment and Authorization lifecycle.

EXIT expects to have completed the relevant policy updates, procedures, and templates in fiscal year 2024. Furthermore, EXIT will coordinate with system owners to schedule contingency planning and disaster recovery activities, such that by the end of fiscal year 2024, all major systems will have been tested within the last 12 months.

Page **4** of **4**

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