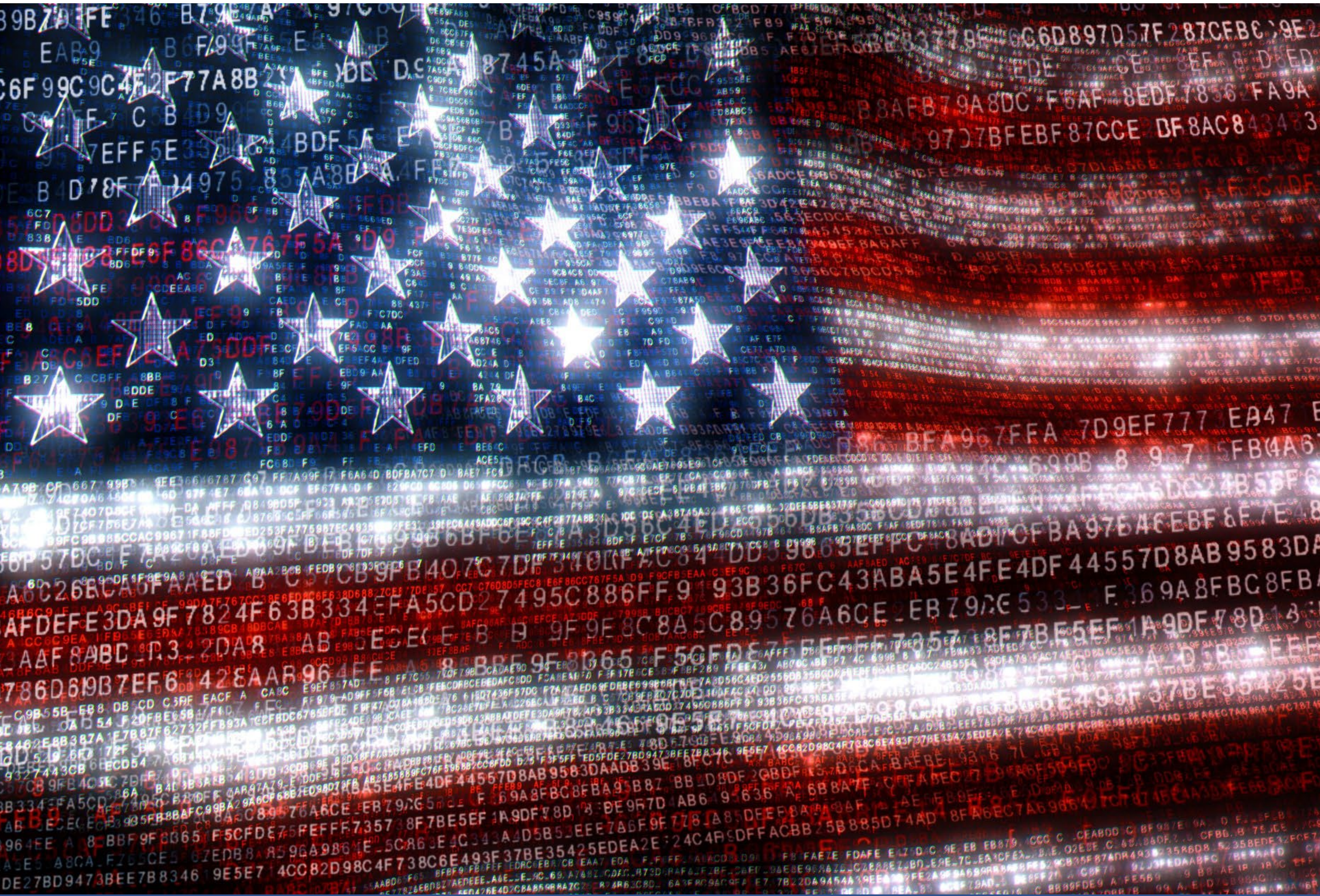
U.S. Consumer Product Safety Commission
OFFICE OF INSPECTOR GENERAL



Evaluation of the CPSC's FISMA Implementation for FY 2022

July 22, 2022

22-A-06

VISION STATEMENT

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

STATEMENT OF PRINCIPLES

We will:

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

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

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

Be innovative, question existing procedures, and suggest improvements.

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

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

Work together to address government-wide issues.

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

July 22, 2022

TO: Alexander Hoehn-Saric, Chair
Dana Baiocco, Commissioner
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: 2022.07.21 15:36:59 -04'00'

SUBJECT: Evaluation of the CPSC's FISMA Implementation for FY 2022

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 and practices. To assess agency compliance with FISMA and to determine the effectiveness of the information security program for fiscal year 2022, 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*.

In evaluating the CPSC's progress in implementing its agency-wide information security program, Williams Adley specifically 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. Although improvements have occurred in some areas, this year's FISMA evaluation found that the CPSC had still not implemented an effective information security program in accordance with FISMA requirements. The lack of an effective Enterprise Risk Management program is a fundamental challenge that the CPSC has faced since we began evaluating FISMA. Establishing effective governance and a formalized approach to managing information security risk is the critical first step to achieving an effective information security program. This is a step the CPSC has repeatedly failed to take.

This year's FISMA report contains 24 recommendations. The CPSC closed six of the recommendations from last year, three new recommendations were made, and 21 recommendations remain open from prior years. Should you have any questions about this report, please contact me.

Table of Contents

Abbreviations and Short Titles

CIGIE	Council of Inspectors General on Integrity and Efficiency
CPSC	U.S. Consumer Product Safety Commission
Cybersecurity Framework	*Framework for Improving Critical Infrastructure Cybersecurity*
DHS	Department of Homeland Security
DPP	Data Protection and Privacy
ERM	Enterprise Risk Management
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IAM	Identity and Access Management
IG	Inspector General
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plans
M	Memorandum
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
Rev.	Revision
SCRM	Supply Chain Risk Management
SP	Special Publication
Williams Adley	Williams, Adley, & Co.-DC LLP

EXECUTIVE SUMMARY

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

FISMA requires the annual evaluation to be performed by the agency's Office of Inspector General (OIG) or by an independent external firm under OIG monitoring. The Office of Management and Budget (OMB) requires OIGs to report their responses to OMB's annual FISMA reporting questions for OIGs via OMB's automated data collection tool, CyberScope. In an effort to streamline the FISMA reporting process and limit the administrative burden on agencies, OMB, in conjunction with the Department of Homeland Security (DHS) and the Council of Inspectors General for Integrity and Efficiency (CIGIE) limited the scope of the evaluation to 20 "core" reporting metrics in fiscal year (FY) 2022.

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 2022 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," considered effective.

WHAT WE FOUND

This year's FISMA evaluation found that the CPSC made progress in implementing FISMA requirements. Specifically, the CPSC closed six recommendations included in the FY 2021 FISMA report that were associated with the core FISMA metrics defined in FY 2022 and completed the following activities:

- Developed a formal process to define and maintain an up-to-date information system inventory.
- Defined the resource designations for a formal Change Control Board.
- Deployed a privileged access management solution.
- Developed data encryption policies and procedures.
- Updated and implemented its incident response policy and plan in accordance with best practices.
- Defined and implemented a process to ensure the timely resolution of incidents.

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. Instead, according to agency management, the CPSC focused its resources and effort on maintaining operational capability, continuing its transition of a portion of the CPSC network to the Cloud, developing new and enhancing existing systems, and responding to government-wide critical security vulnerabilities and emergency directives from the DHS. Agency management further stated it expended resources on planning, managing budgets, and coordinating procurements.

In order to achieve effective information security, the CPSC must prioritize the improvement of its information technology security program by establishing robust enterprise information security risk management practices. In commenting on a draft of this report, management provided a response, which is presented in Appendix B. We did not evaluate management's response and, accordingly, we express no opinion on the response.

WHAT WE RECOMMEND

To improve the CPSC's implementation of FISMA, we made 24 recommendations that the CPSC must address in order to mature its information security program. We provided 3 new recommendations and reissued 21 prior year recommendations related to 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 2022.

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)-22-05, *Fiscal Year 2021-2022 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 related in-scope IG FISMA domains except for the Respond domain. Specifically, we identified 20 specific deficiencies across 8 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 24 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 (21) were based on prior year deficiencies; there were 3 new recommendations.

Federal Information Security Modernization Act of 2014

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

National Institute of Standards and Technology (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 (NIST 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

[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.

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

- **Identify –** The identify function requires the development of organizational understanding 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 action 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 2022 Reporting Metrics

The FY 2022 IG FISMA Reporting Metrics identified 20 core metrics and were developed by OMB, DHS, and CIGIE and incorporated the NIST Framework's five (5) information security functions to 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 strategy at all levels of the organization; as well as monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its risk management program.

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

2. Protect Function

○ *Configuration Management* – An agency with an effective configuration management program employs automation to maintain an accurate view of the security configurations for all information system components connected to the agency's network; consistently implements its configuration management policies, procedures, plans, and strategy 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 mature 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 definitions of the five levels of the maturity model spectrum below:

- **Level 1: Ad hoc** – Policies, procedures, and strategy are not formalized; activities are performed in an ad hoc, reactive manner.
- **Level 2: Defined** – Policies, procedures, and strategy are formalized and documented but not consistently implemented.
- **Level 3: Consistently Implemented** – Policies, procedures, and strategy 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 strategy are collected across the organization and

[5] CIGIE, DHS, OMB, "FY22 Core IG Metrics Implementation Analysis and Guidelines" https://www.cisa.gov/sites/default/files/publications/CIGIE%20FY22%20Core%20Metrics%20Implementation%20Analysis%20and%20Guidelines-final.pdf.

used to assess them and make necessary changes.

- **Level 5: Optimized** – Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Key Changes to the IG FISMA Reporting Metrics in FY 2022

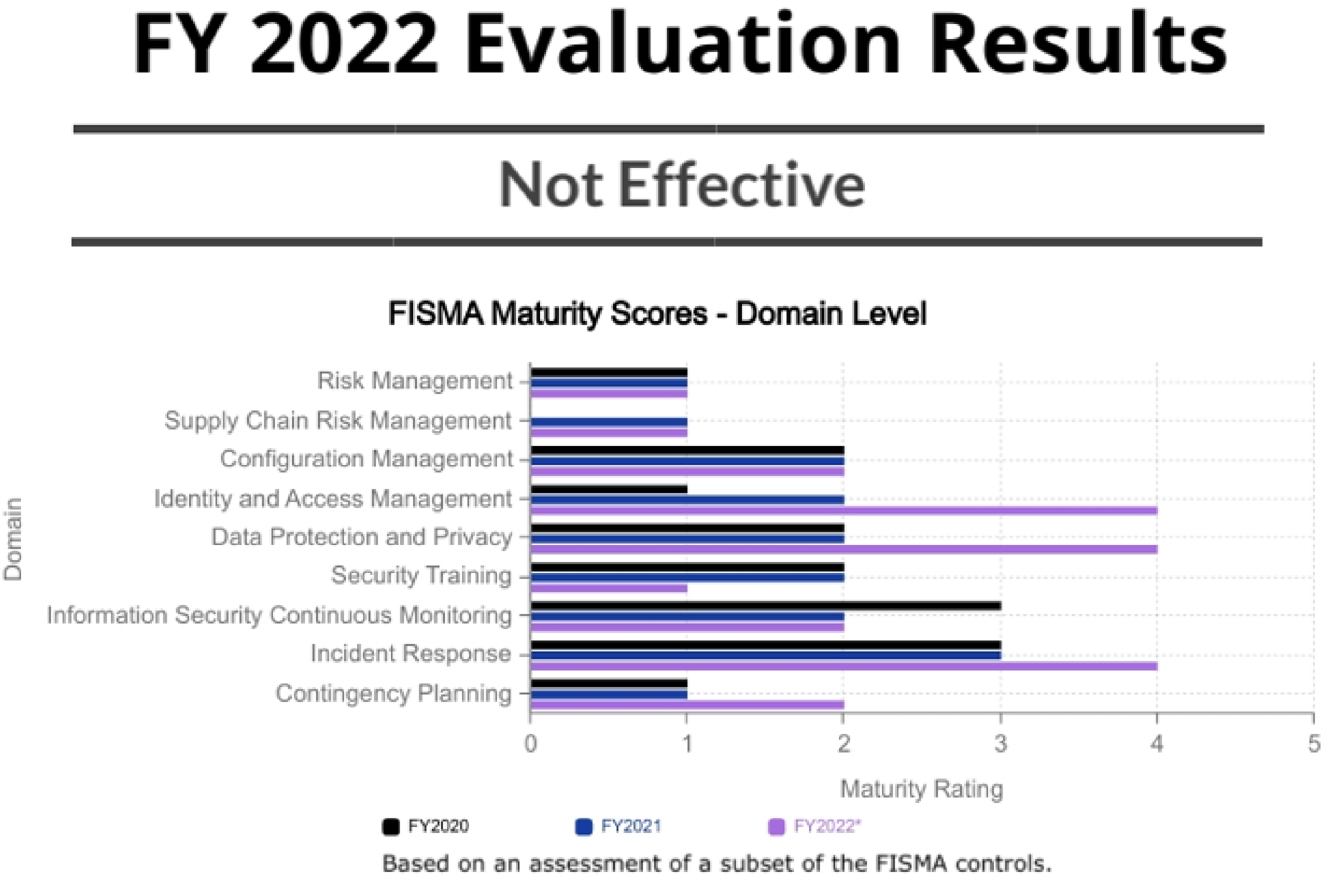
According to the IG FISMA metrics, one of the goals of the annual FISMA evaluation is to assess agencies' progress toward achieving outcomes that strengthen federal cybersecurity, including implementing the administration's priorities and best practices. The FY 2022 FISMA IG metrics focused on 20 core IG metrics and did not include the full suite of 66 metrics from the prior year. The FY 2022 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, including:

- *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (OMB M-22-09) – The goal of which is to accelerate agencies towards a baseline of early zero trust maturity.
- *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (OMB M-21-31) – This memorandum provides specific requirements for log management and includes a maturity model, prioritizing the most critical log types and requirements.
- *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* (OMB M-22-01) – This memorandum requires agencies to focus on improving early detection capabilities, creating "enterprise-level visibility" across components and sub-agencies, and deploying an Endpoint Detection and Response solution.

Williams Adley utilized the criteria established by the federal government to evaluate the CPSC's FY 2022 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 2022.



*based on FY2022 review of FY2020 core metrics

Figure 3-1. FY 2022 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 except for the Incident Response domain. Each of the related conditions and supporting criteria are documented in the function sections below.

Root Cause

The CPSC information security program was not effective because the CPSC has still 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 Enterprise Risk Management (ERM) program have not been developed. The CPSC Office of Information and Technology Services is responsible for managing and implementing the CPSC's information security program and related practices. However, the CPSC's ERM program is not sufficiently defined, and the Office of Information and Technology Services has not received specific direction from the ERM program about how to integrate information security risk, including supply chain risks, into organization-wide risk management practices. Williams Adley reported the lack of an ERM program in both FY 2020 and FY 2021.

CPSC management asserts that it has not addressed previously identified information security deficiencies due to competing priorities. The number of competing priorities for the CPSC amplifies the need for the CPSC to leverage ERM to prioritize identified information security deficiencies and their related recommendations as 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 in the corresponding section. A majority of the recommendations (24) identified below are directly related to prior year deficiencies and recommendations, while three (3) of the recommendations identified below are new this year as indicated by the parenthetical reference "(2022 recommendation)."

4.1 Identify Function Area

Progress

In FY 2022, the CPSC made progress in addressing previously identified Risk Management deficiencies. For example, the CPSC has defined the Information System Registration & Inventory Procedures, which closed a prior year recommendation. Furthermore, according to the Office of Financial Management, Planning and Evaluation, the CPSC is currently implementing a corrective action plan for the Federal Managers' Financial Integrity Act audit report and will integrate ERM as part of the CPSC's development and review of internal controls. Overall, the CPSC has made progress on open prior year recommendations, but not enough to close any findings.

Risk Management Conditions

Williams Adley determined that the CPSC was operating at Maturity Level 1- Ad hoc 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 its newly developed Information System Registration & Inventory Procedures.

ii. The CPSC has not fully defined system boundaries.

iii. 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.

iv. 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.

v. 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

vi. 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 previously identified SCRM deficiencies in FY 2022. For example, the CPSC has defined an SCRM policy. However, 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 the 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.

Identify Function Recommendations

1. Implement registration and inventorying procedures for 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 2020 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 (ERM) program based on National Institute of Standards and Technology and ERM Playbook (OMB Circular A-123, Section II requirement) guidance. This includes establishing a cross-departmental risk executive (function) lead 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 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*).
11. Develop supply chain risk management procedures to ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain risk management requirements (*Supply Chain Risk Management 2021 Recommendation*).

4.2 Protect Function Area

Progress

The CPSC has made progress in addressing the previously identified Configuration Management deficiencies in FY 2022. For example, the CPSC closed a prior year recommendation by establishing a Change Control Board Charter which formalized the roles and responsibilities of the Change Control Board members. 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 (IAM) deficiencies in FY 2022. For example, the CPSC has implemented a user account management system for privileged user access. All privileged user access is managed with this tool except one database account.

Furthermore, the CPSC made progress in addressing previously identified Data Protection and Privacy (DPP) deficiencies in FY 2022. The CPSC has developed policies for the encryption of data-at-rest in tandem with data-in-transit in accordance with NIST recommendations. The CPSC has also developed a new policy and procedures for sanitization of digital media prior to disposal or reuse.

Configuration Management Conditions

Williams Adley determined that the CPSC was operating at Maturity Level 2 - Defined for the configuration management IG FISMA metric domain. An effective configuration management program is critical to identify and mitigate vulnerabilities that can be exploited within the CPSC's environment. By not taking the strategic steps to develop and implement proper configuration plans and procedures, unknown risks and vulnerabilities may be introduced by new or existing products, system components, systems, and services of external providers. Williams Adley identified the following deficiencies within the configuration management IG FISMA metric domain:

i. The CPSC has 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.
ii. The CPSC has not established procedures for documenting, managing, and monitoring deviations from agreed upon configuration settings.
iii. 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.

Identity and Access Management Conditions

Williams Adley determined that the CPSC was operating at Maturity Level 4 – Managed and Measurable for the IAM IG FISMA metric domain. An effective IAM program is critical to prevent unauthorized system access. Although the CPSC scored Level 4 – Managed and Measurable by meeting the FISMA effectiveness goal, 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 the CPSC's systems is increased. Unauthorized access may result in improper access to and dissemination of confidential data, and other malicious activities. Williams Adley identified the following deficiencies within the IAM IG FISMA metric domain:

i. The CPSC has not defined its processes for provisioning, managing, and reviewing privileged accounts.
ii. The CPSC does not log and actively monitor activities performed while using privileged access that permit potentially incompatible duties.

Data Protection and Privacy Conditions

Williams Adley determined that the CPSC was operating at Maturity Level 4 – Managed and Measurable for the DPP IG FISMA metric domain. An effective DPP program is critical to protect PII and prevent data loss. Although the CPSC scored Level 4 – Managed and Measurable meeting the FISMA effectiveness target, Williams Adley identified deficiencies that impact the overall effectiveness of the information security program. 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 consistently implemented policies and procedures for encryption of data at rest, encryption of data in transit, and sanitization of digital media.

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. 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 Security Training IG FISMA metric domain:

i. The CPSC has defined training requirements for certain information security roles. However, 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.

Protect Function Recommendations

We recommend that the CPSC:

12. 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*).

13. Integrate the management of secure configurations into the organizational configuration management process *(Configuration Management 2020 Recommendation)*.
14. Develop and implement policies and procedures in support of Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploitable Vulnerabilities, (Configuration Management 2020 Recommendation - Modified).*
15. Log and actively monitor activities performed while using privileged access that permit potentially incompatible duties (*Identity and Access Management 2020 Recommendation)*
16. Define and implement processes for provisioning, managing, and reviewing privileged accounts (*Identity and Access Management 2021 Recommendation*).
17. Implement data encryption and sanitization of digital media policies and procedures (*Data Protection & Privacy 2020 Recommendation – Modified*).
18. Perform an assessment of the knowledge, skills, and abilities of CPSC personnel with significant security responsibilities (*Security Training 2020 Recommendation*).

4.3 Detect Function

Progress

In FY 2022, the CPSC made progress in addressing previously identified Information Security Continuous Monitoring (ISCM) deficiencies. For example, the CPSC maintained valid Authorizations to Operate packages for the General Support System Local Area Network, General Support System Cloud, Consumer Product Safety Risk Management System, International Trade Data System/Risk Assessment Methodology, and Office 365.

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 CPSC has not implemented an ISCM program that supports a Risk Management Program designed in accordance with NIST guidance to support each organizational tier, specifically the business unit and enterprise-wide tiers. For example, according to NIST, organizational risk tolerance should drive the ISCM strategy and based on documentation provided, the CPSC has not leveraged any explicit risk tolerance to drive the ISCM program.
ii. System Security Plans for sampled systems included information that is out-of-date.
iii. The CPSC has not assessed 60 out of its 79 identified minor applications since 2018. Further, the CPSC has never assessed 8 of these applications.

Detect Function Recommendations

We recommend that the CPSC:

19. Integrate the established strategy for identifying organizational risk tolerance into the Information Security Continuous Monitoring plan *(Information Security Continuous Monitoring 2020 recommendation)*.
20. Update the System Security Plans to include the most up-to-date information and assess the relevant minor applications *(Information Security Continuous Monitoring 2022 recommendation).*

4.4 Respond Function

Progress

In FY 2022, the CPSC made progress in addressing previously identified Incident Response deficiencies. For example, the CPSC has migrated to a new Security Event and Incident Management tool to improve log aggregation and alerting, as well as to improve integration with the CPSC's other incident response tools. The CPSC also utilizes profiling techniques to baseline expected activities on its networks and systems, so that it can more effectively detect security incidents and meet performance metrics. Williams Adley has determined that the CPSC was operating at Maturity Level 4 – Managed and Measurable for the overall maturity level of the CPSC's Incident Response FISMA metric domain. Williams Adley did not issue any recommendations in FY 2022 for the Incident Response domain.

4.5 Recover Function

Progress

In FY 2022, the CPSC made some progress in addressing previously identified Contingency Planning deficiencies. For example, the CPSC completed the Information System Contingency Plan (ISCP) tests for the General Support System Local Area Network, Consumer Product Safety Risk Management System, and International Trade Day System/Risk Assessment Methodology in FY 2021. However, the CPSC had not performed the ISCP tests in FY 2022 at the time of this assessment for all sampled information systems. This is because the CPSC tests its ISCPs on an annual basis in accordance with agency policy and the next tests were not scheduled for completion until September 2022. Therefore, the results of these tests were not available for Williams Adley to review.

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. Prior to FY 2021, the CPSC surveyed some of the CPSC program offices to aid them in identifying critical systems while completing the General Support System Business Impact Assessment. However, the Business Impact Assessment does not define the CPSC's mission essential functions. Further, the Business Impact Assessment states that recovery timing requirements may not be adequate for at least two major applications. In addition, the CPSC has not developed the other contingency planning documents required to support a comprehensive Continuity of Operations Plan, such as a Disaster Recovery Plan.
ii. The CPSC has not developed all of the contingency planning documents required to support a comprehensive Continuity of Operations Plan, such as a Disaster Recovery Plan and Business Continuity Plans.
iii. The CPSC has not completed ISCP testing for three (3) out of five (5) sampled major systems.

Recover Function Recommendations

We recommend that the CPSC:

21. Develop and document a robust and formal approach to contingency planning for agency systems and processes that include mission essential functions using the appropriate guidance (e.g., NIST SP 800-34/53, Federal Continuity Directive 1, NIST Cybersecurity Framework, and National Archive and Records Administration guidance) *(Contingency Planning 2020 Recommendation*).
22. Develop, document, and distribute all required Contingency Planning documents (ex. organization-wide Continuity of Operation Plan and Business Impact Assessment, Disaster Recovery Plan, Business Continuity Plans, in accordance with appropriate federal and best practice guidance *(Contingency Planning 2020 Recommendation*).
23. Integrate documented contingency plans with the other relevant agency planning areas *(Contingency Planning 2020 Recommendation*).
24. Test the set of documented contingency plans *(Contingency Planning 2020 Recommendation - Modified).*

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. *(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 *(2020 Recommendation)*. 3. Establish and implement a policy and procedures to manage software licenses using automated monitoring and expiration notifications *(2020 Recommendation*). 4. Establish and implement a policy and procedure to ensure that only authorized hardware and software execute on the agency's network *(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) *(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 *(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 *(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 *(2020 Recommendation*). 9. Develop and implement an Enterprise Risk Management

	(ERM) program based on National Institute of Standards and Technology and ERM Playbook (OMB Circular A-123, Section II requirement) guidance. This includes establishing a cross-departmental risk executive (function) lead by senior management to provide both a departmental and organization level view of risk to the top decision makers within the CPSC *(2020 Recommendation*). 10. 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 *(2022 Recommendation*).
Identify(Supply Chain Risk Management)	11. Develop supply chain risk management procedures to ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain risk management requirements *(2021 Recommendation)*.
Protect(Configuration Management)	12. 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 (*2020 Recommendation*). 13. Integrate the management of secure configurations into the organizational configuration management process *(2020 Recommendation)*. 14. Develop and implement policies and procedures in support of Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploitable Vulnerabilities* (*2020 Recommendation - Modified*).
Protect(Identity and Access Management)	15. Log and actively monitor activities performed while using privileged access that permit potentially incompatible duties *(2020 Recommendation*). 16. Define and implement processes for provisioning, managing, and reviewing privileged accounts *(2021 Recommendation*).
Protect(Data Protection and Privacy)	17. Implement data encryption and sanitization of digital media policies and procedures *(2020 Recommendation - Modified*).
Protect(Security Training)	18. Perform an assessment of the knowledge, skills, and abilities of CPSC personnel with significant security responsibilities *(2020 Recommendation*).
Detect(Information Security Continuous Monitoring)	19. Integrate the established strategy for identifying organizational risk tolerance into the Information System Configuration Management plan *(2020 recommendation*).

	20. Update the System Security Plans to include the most up-to-date information and assess the relevant minor applications *(2022 recommendation*).
Recover(Contingency Planning)	21. Develop and document a robust and formal approach to contingency planning for agency systems and processes that include mission essential functions using the appropriate guidance (e.g., NIST SP 800-34/53, Federal Continuity Directive 1, NIST Cybersecurity Framework, and National Archive and Records Administration guidance) *(2020 Recommendation*). 22. Develop, document, and distribute all required Contingency Planning documents (ex. organization-wide Continuity of Operation Plan and Business Impact Assessment, Disaster Recovery Plan, Business Continuity Plans, in accordance with appropriate federal and best practice guidance *(Contingency Planning 2020 Recommendation*). 23. Integrate documented contingency plans with the other relevant agency planning areas *(2020 Recommendation).* 24. Test the set of documented contingency plans (*2020 Recommendation - Modified*).

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 2022. In support of this objective, Williams Adley conducted the evaluation in accordance with OMB M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements,* reporting guidelines.

A.2 Scope

The evaluation focused on reviewing the CPSC's implementation of FISMA for FY 2022 based on OMB M-22-05. The FISMA evaluation covered the period of October 1, 2021, to June 30, 2022. 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. Five major CPSC information systems were selected rotationally based on risk for the evaluation:

- General Support System Local Area Network
- General Support System Cloud
- Consumer Product Safety Risk Management System
- Office 365
- International Trade Data System/Risk Assessment Methodology System

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 2022 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

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

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 2022 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. Code, section 3555(j).

We performed this evaluation from March through June 2022 and conducted this evaluation in accordance with CIGIE *Quality Standards for Inspection and Evaluation*. Those standards require that we obtain sufficient evidence to provide a reasonable basis for our findings and conclusions 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 on July 6, 2022.

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 2022 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 judgment, 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 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.

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

- Center for Internet Security *Top 18 Security Controls*
- Chief Information Officer Council/Chief Acquisition Officer Council, *Cloud Computing Contract Best Practices*
- Cybersecurity and Infrastructure Security Agency, *Cybersecurity & Incident Response Playbooks*
- Cybersecurity and Infrastructure Security Agency, *Cybersecurity Incident and Vulnerability Response Playbooks*
- Cybersecurity and Infrastructure Security Agency, *Zero Trust Maturity Model*
- Department of Homeland Security Binding Operational Directive 18-02
- Department of Homeland Security Binding Operational Directive 19-02
- Department of Homeland Security Binding Operational Directive 22-01
- Department of Homeland Security Emergency Directive 19-01
- Department of Homeland Security Fiscal Year 2022 Chief Information Officer Federal Information Security Modernization Act Metrics
- Executive Order 13636
- Executive Order 13800
- 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 199
- Federal Information Processing Standards 201-2
- Federal Risk and Authorization Management Program - Standard Contract Clauses
- Homeland Security Presidential Directive 12
- National Cybersecurity Workforce Framework
- National Institute of Standards and Technology Cybersecurity Framework
- National Institute of Standards and Technology Interagency or Internal Report 8011
- National Institute of Standards and Technology Interagency or Internal Report 8276
- National Institute of Standards and Technology Interagency or Internal Report 8286
- National Institute of Standards and Technology SP 800-18
- National Institute of Standards and Technology SP 800-34

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

- National Institute of Standards and Technology SP 800-37, Rev. 2
- National Institute of Standards and Technology SP 800-39
- National Institute of Standards and Technology SP 800-40, Rev. 3
- National Institute of Standards and Technology SP 800-50
- National Institute of Standards and Technology SP 800-53, Rev. 5
- National Institute of Standards and Technology SP 800-61, Rev. 2
- National Institute of Standards and Technology SP 800-63
- National Institute of Standards and Technology SP 800-70, Rev. 4
- National Institute of Standards and Technology SP 800-128
- National Institute of Standards and Technology SP 800-137
- National Institute of Standards and Technology SP 800-152
- National Institute of Standards and Technology SP 800-157
- National Institute of Standards and Technology SP 800-181
- National Institute of Standards and Technology SP 800-207
- National Institute of Standards and Technology SP 800-218
- Office of Management and Budget Circular No. A-123
- Office of Management and Budget Circular No. A-130
- Office of Management and Budget Memorandum 14-03
- Office of Management and Budget Memorandum 16-17
- Office of Management and Budget Memorandum 17-25
- Office of Management and Budget Memorandum 19-03
- Office of Management and Budget Memorandum 19-17
- Office of Management and Budget Memorandum 20-04
- Office of Management and Budget Memorandum 21-07
- Office of Management and Budget Memorandum 21-30
- Office of Management and Budget Memorandum 21-31
- Office of Management and Budget Memorandum 22-01
- Office of Management and Budget Memorandum 22-05
- Office of Management and Budget Memorandum 22-09
- US-Computer Emergency Readiness Team, *Incident Response Guidelines*

Appendix B: Management Response

From: Rolfes, James <JRolfes@cpsc.gov>
Sent: Thursday, July 21, 2022 2:23 PM
To: Chatly, Ankit <AChatly@cpsc.gov>; Levine, Jason <JLevine@cpsc.gov>
Cc: Manley, Patrick <pmanley@cpsc.gov>; Dentel, Christopher <CDentel@cpsc.gov>; Burrows, Daniel <DBurrows@cpsc.gov>; Meier, Mary <MMeier@cpsc.gov>; Hennessy, Kieran <KHennessy@cpsc.gov>; Reeser, Kyle <KReeser@cpsc.gov>
Subject: RE: FY2022 Draft CPSC FISMA Report

Ankit,

Here’s our management response.

Management generally concurs with the OIG FISMA Evaluation for FY 2022.

Regards,

Jim Rolfes
Chief Information Officer and Chief Data Officer
U.S. Consumer Product Safety Commission

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

To report Fraud, Waste, or Abuse, Mismanagement, or Wrongdoing at the CPSC go to
OIG.CPSC.GOV or call (301) 504-7906

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