Office of Inspector General

U.S. Consumer Product Safety Commission

Evaluation of CPSC's FISMA Implementation for FY 2020

November 3, 2020

Report 21-A-01

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.

November 3, 2020

TO: Robert S. Adler, Acting Chairman
Elliot F. Kaye, Commissioner
Dana Baiocco, Commissioner
Peter A. Feldman, Commissioner

FROM: Christopher W. Dentel, Inspector General

SUBJECT: Evaluation of CPSC's FISMA Implementation for FY 2020

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 FY 2020, 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 an evaluation 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.

This year's FISMA evaluation found that although management continues to make progress in implementing the FISMA requirements much work remains to be done. A fundamental challenge facing the CPSC is its failure to implement an effective Enterprise Risk Management program. Establishing effective governance and a formalized approach to information security risk management is the critical first step to achieving an effective information security program.

There are 47 recommendations in this year's FISMA review. These recommendations and the areas identified as requiring improvement are detailed in the attached report. Should you have any questions, please contact me.

Table of Contents

Executive Summary

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

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 Fiscal Year (FY) 2020 and to determine the effectiveness of the information security program. This report documents the results of the FISMA evaluation. In evaluating the CPSC's progress in implementing its agency-wide information security program, we specifically assessed the CPSC's compliance with the annual Inspector General (IG) FISMA reporting metrics set forth by the Department of Homeland Security (DHS) and OMB. FISMA metrics require that in order to achieve an effective information security program an agency must first establish and define sound policies, procedures, and practices.

What We Found

This year's FISMA evaluation found that the CPSC continues to make progress in implementing the FISMA requirements. For example, the CPSC has closed 15 recommendations included in the FY 2019 FISMA report, and the CPSC has:

- Continued development of a formal Enterprise Architecture
- Made progress on completing Plans of Actions & Milestones
- Continued the implementation of technology to support privileged user account management
- Hired an additional person to support the privacy program
- Continued the implementation of Information Security Continuous Monitoring (ISCM) program system level requirements
- Further enhanced network defenses by baselining network activity through the use of network profiling techniques
- Performed some business impact analysis tasks to enhance contingency planning

However, we determined that the CPSC has not implemented an effective information security program in accordance with FISMA requirements. The CPSC did not implement an effective program because the CPSC does not have a formal approach to information security risk management and has not defined a sufficient approach to utilize its limited resources. The CPSC must continue to prioritize the improvement of its program in order to achieve effective information security.

What We Recommend

To improve the CPSC's implementation of FISMA, we made 47 recommendations that the CPSC must address in order to mature its information security program. We modified 2 existing recommendations and provided 7 new recommendations, with 2 key recommendations related to improving the CPSC information security risk management practices, and reissued 38 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 2020.

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, including an annual independent evaluation of an agency's information security program and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. The evaluation also must include an assessment of the effectiveness of the information security policies, procedures, and practices of the agency as a whole. FISMA requires the annual evaluation to be performed by the agency's OIG or by an independent external firm under OIG supervision. OMB Memorandum 20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*, dated November 19, 2019, requires the OIG to report their responses to OMB's annual FISMA reporting questions for OIGs via CyberScope.

The CPSC OIG retained Williams Adley to perform an independent evaluation of the CPSC's implementation of FISMA for FY 2020. This report presents the results of that independent evaluation. Williams Adley will also prepare responses to OMB's annual FISMA reporting questions for OIGs, and the CPSC OIG will submit this information via OMB's automated collection tool in accordance with OMB guidance.

Federal Information Security Modernization Act of 2014

The requirements of the Federal Information Security Management Act of 2002 were updated with the passage of the Federal Information Security Modernization Act of 2014. 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 to take a risk-based approach to protecting their information and information systems and addressing their unique

cybersecurity challenges.

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. Resulting from this Executive Order was National Institute of Standards and Technology's (NIST) "Framework for Improving Critical Infrastructure Cybersecurity [Cybersecurity Framework]."[2] The Cybersecurity Framework[3] provides guidelines for organizations to protect critical infrastructure[4] 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[5] was issued to hold agency heads accountable for managing cybersecurity risk in their organizations. Specifically, Executive Order 13800 defines effective risk management as requiring agency heads to lead integrated teams of senior executives with expertise in information technology (IT), 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 hold 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 to address those risks. The Cybersecurity Framework contains five information security functions that give federal agencies the ability to select and prioritize improvements in information security risk management. The five information security functions are as follows:

- **Identify** – The "identify" function requires the development of organizational understanding to manage information security risk to systems,

[1] Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," February 12, 2013.
[2] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," February 12, 2014.
[3] 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.
[4] 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."
[5] Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017.

assets, data, and capabilities. The activities in the "identify" function are foundational for effective use 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 govern 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 preceding it. For example, an organization cannot *protect* its IT environment correctly 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.

Reporting Metrics

FISMA requires OMB to ensure that guidance is developed for the independent evaluation of agency information security programs. On April 17, 2020, OMB, DHS, and the Council of Inspectors General on Integrity and Efficiency (CIGIE) released the "FY 2020 IG Federal Information Security Modernization Act of 2014

Reporting Metrics."[6] This guidance provides metrics to be used to gauge the maturity of agency practices in connection with the eight IG FISMA metric domains that are organized around the five information security functions outlined in the Cybersecurity Framework:

- **Identify**
  - *Risk Management* - The purpose of the risk management IG FISMA metric domain is to evaluate the maturity of an agency's risk management program. 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; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its risk management program.
- **Protect**
  - *Configuration Management* – The purpose of the configuration management IG FISMA metric domain is to evaluate the maturity of an agency's configuration management program. 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* – The purpose of the identity and access management IG FISMA metric domain is to evaluate the maturity of an agency's identity and access management program. 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* – The purpose of the security training IG FISMA metric domain is to evaluate the maturity of an agency's security training program. An agency with an effective security training program addresses all of its identified knowledge, skills, and abilities gaps; measures the effectiveness of its security awareness and training program; and ensures that staff are consistently collecting, monitoring, and analyzing qualitative and quantitative

[6] OMB, DHS, and CIGIE, "FY 2020 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics," April 17, 2020.

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

o *Data Protection and Privacy* – The purpose of the Data Protection and Privacy IG FISMA metric domain is to evaluate the maturity of an agency's data protection and privacy program. 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.

- **Detect**

o *Information Security Continuous Monitoring* – The purpose of the information security continuous monitoring IG FISMA metric domain is to evaluate the maturity of an agency's information security continuous monitoring program. 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.

- **Respond**

o *Incident Response* – The purpose of the incident response IG FISMA metric domain is to evaluate the maturity of an agency's incident response program. 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.

- **Recover**

o *Contingency Planning* – The purpose of the contingency planning IG FISMA metric domain is to evaluate the maturity of an agency's contingency planning program. An agency with an effective contingency planning program employs automated mechanisms to more 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.

NIST Risk Management Framework

NIST has established the information security risk management best practices via the Risk Management Framework as detailed in the Special Publication (SP) 800-37, Revision (Rev) 2, *Risk Management Framework for Information Systems and Organizations*,[7] and NIST SP 800-39, *Managing Information Security Risk*.[8] 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.

Maturity Models

According to the IG FISMA metrics, the effectiveness of an information security program is determined based on the ratings earned on a maturity model spectrum, which identifies whether an agency has developed policies and procedures, implemented documented processes, and established methods to improve over time. The maturity model spectrum is divided into five levels outlined 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 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

According to the FY 2020 IG FISMA metrics, "a Level 4, Managed and Measurable, information security program is operating at an effective level of security. Generally, a Level 4 maturity level is defined as formalized, documented, and

[7] NIST SP 800-37, Managing Information Security Risk: Organization, Mission, and Information System View," March 2011.
[8] NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View," March 2011.

consistently implemented policies, procedures, and strategies and where quantitative and qualitative performance measures on the effectiveness of said policies, procedures, and strategies are collected across the organization and assessed to make necessary changes."

Williams Adley utilized the criteria established by the federal government to evaluate the CPSC's FY 2020 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 continued to make improvements to its information security program and made progress in implementing some of the recommendations resulting from previous FISMA evaluations, the CPSC has not implemented an effective information security program in FY 2020.

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

Overall, based on the evaluation procedures performed, Williams Adley has 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 a number of deficiencies for each of the related in-scope IG FISMA Metric domains. Each of the related conditions and supporting criteria are documented in the sections below.

Cause

The CPSC information security program was not effective because the CPSC 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. Although the CPSC has begun to develop an Enterprise Risk Management (ERM) program to guide risk management practices at the CPSC, explicit guidance and processes to address information security risks and integrate those risks into the broader agency-wide ERM program has not been developed. In addition, the CPSC has not leveraged the relevant information security risk management guidance prescribed by NIST to develop an approach to manage information security risk. Further, as asserted by CPSC personnel, the CPSC has limited resources to operate the information security program and to address the extensive FISMA requirements and related complex cybersecurity challenges. Therefore, the CPSC has not dedicated the resources necessary to fully address these challenges and requirements. The CPSC began addressing previously identified information security deficiencies but was not able to address all deficiencies in FY 2020.

The CPSC Office of Information Technology (EXIT) is responsible for managing and implementing the CPSC information security program and related practices. However, EXIT has not received specific direction from the ERM program about how to prioritize information security risks within a mission and organizational framework. EXIT has not been given any explicit guidance on how to establish and use risk tolerance to make risk-based decisions based on best practice guidance established by NIST. Based on inquiries with CPSC personnel, EXIT continues to wait for guidance from the ERM group to decide how to approach new information security risk management requirements. However that guidance has not yet been provided and the CPSC has not developed an explicit strategy to address information security risks in accordance with NIST requirements. If the CPSC is to implement an effective information security program as required by FISMA, the CPSC must first develop and then implement an information security risk management strategy in accordance with NIST guidance.

CPSC personnel assert limited resources continue to make it difficult to address

previously identified information security program deficiencies while also meeting the demands of continuously emerging cybersecurity challenges. Going forward managing the information security program most likely will continue to be a challenge for the CPSC due to limited resources available. Therefore, directing those limited resources and prioritizing information security tasks, with direction and guidance from the ERM program, is imperative and will only become more important as cybersecurity challenges become more and more sophisticated.

Further, in FY 2019, the CPSC received 55 recommendations to address identified information security deficiencies. Although the CPSC made progress in completing some of the agreed upon recommendations, the CPSC asserted that it did not have sufficient resources to address all the recommendations. Once the CPSC develops a formal information security risk management strategy, the CPSC must utilize these risk management practices to direct resources to address priority deficiencies. The creation of a detailed corrective action plan that lists and prioritizes recommendations will also be required.

Effect

Due to the nature of the deficiencies identified and given the large amount of sensitive data handled by the CPSC, Williams Adley is concerned with the strength of the existing information security program. It is critical that the CPSC implement an effective information security program to secure data that is stored, processed, and/or transmitted by the CPSC. A data breach at the CPSC has 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, can 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 mission or business risk and thus implementation of an effective information security program needs to be prioritized.

Recommendations

The following recommendations are key recommendations that the CPSC must implement in order to take the most critical steps to mature its information security program. However, we recognize that the CPSC must also address the individual conditions presented in each IG FISMA metric domain and, as such, have provided a list of recommendations associated with each relevant condition in the corresponding section.

Some of the conditions identified below are directly related to prior year deficiencies, as indicated by the following parenthetical reference "(prior year recommendation)," and some of the conditions identified below are new this year as indicated by the following parenthetical reference "(2020 recommendation)."

We offer the following key recommendations to address the cause identified:

FY 2020 Root-Cause Recommendations:

1. Develop and implement a formal strategy to address information security risk management requirements as prescribed by the National Institute of Standards and Technology guidance (*prior year recommendation – modified*).
2. 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 (*prior year recommendation – modified*).

We offer the following new recommendations:

FY 2020 Additional Recommendations:

3. Develop and implement a process to maintain an up-to-date and complete information system inventory.
4. Develop and implement an information security architecture that supports the CPSC Enterprise Architecture and is integrated into the agency's Enterprise Risk Management Program.
5. Consistently implement [redacted], including the remediation of [redacted].
6. Develop and implement a process to ensure the completion of access agreements for all CPSC information system users.
7. Develop and implement data encryption policies and procedures.
8. Define and implement Information Security Continuous Monitoring (ISCM) procedures, to include the monitoring of performance measures, that support the updated ISCM plan.
9. Update and implement the CPSC Incident Response (IR) Policy and IR Plan with latest practices, including IR performance measures and the latest implemented network profiling techniques.

4.1 Risk Management

Conditions

In FY 2020, the CPSC made progress in addressing previously identified risk management deficiencies. For example, the CPSC made progress on completing several Plans of Actions & Milestones and continued the development of comprehensive Enterprise Architecture. However, based on evaluation procedures performed, Williams Adley identified the following deficiencies within the Risk Management IG FISMA metric domain:

i. The CPSC has not fully defined a process for developing and maintaining a comprehensive and accurate inventory of its information systems. Specifically, the CPSC does not have defined processes to register an information system for purposes of management, accountability, coordination, and oversight of information systems, or defined requirements/processes for maintaining an inventory of information systems.

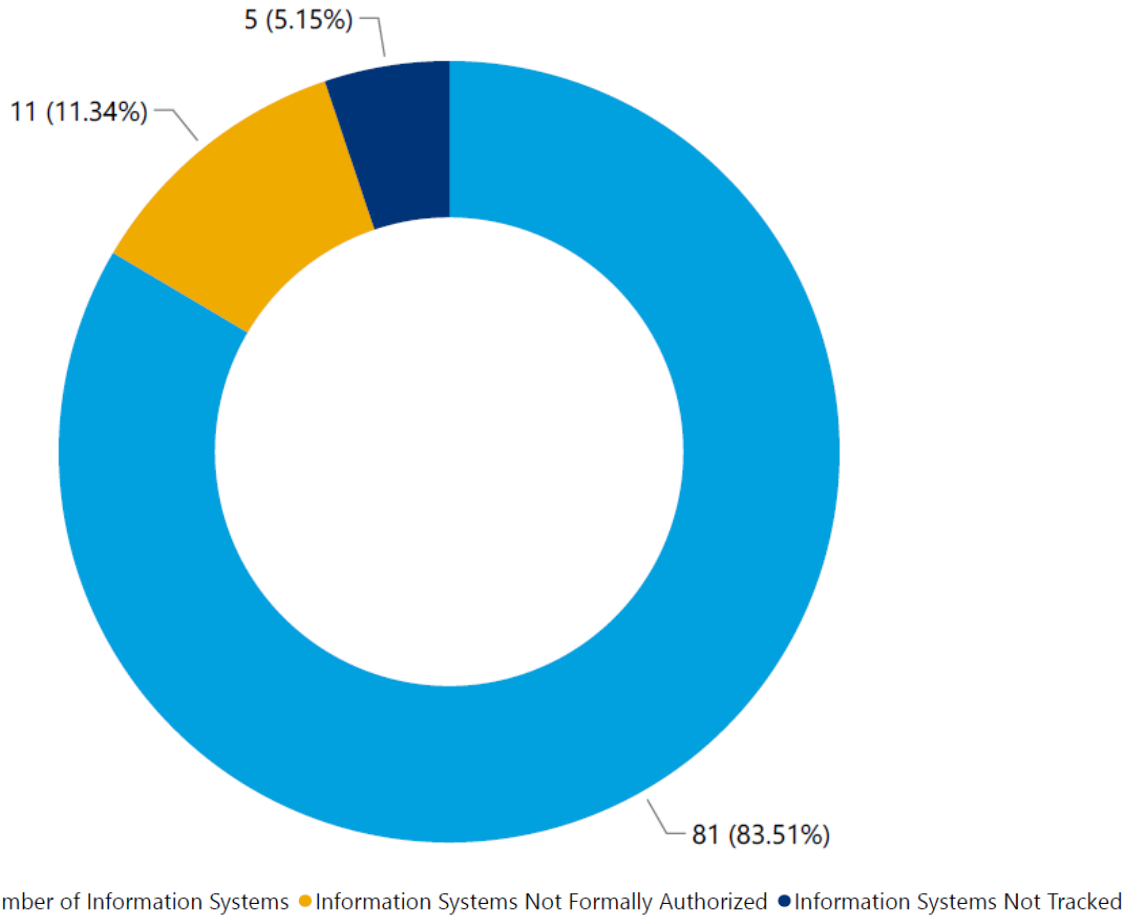
Information System Inventory

In coordination with the OIG, 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. 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 a 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 11 information systems that were not authorized, 5 information systems that were not tracked, and 81 information systems that were known, authorized, and tracked.

Figure 4-1. Information System Inventory Analysis



We met with EXIT to confirm the results of the analysis presented above. Although EXIT acknowledged that the information system inventory provided to us for evaluation was out-of-date and has since been updated, it is likely that, due to the lack of procedures guiding this process and the lack of coordination between CPSC departments, deficiencies exist within the current official CPSC information system inventory and an internal analysis should be performed to identify and remediate these gaps.

Additional risk management conditions include:

ii. The CPSC has not developed a process for using standard data elements/taxonomy to [redacted] with the detailed information necessary for tracking and reporting.

iii. The CPSC has not developed a process for using standard data elements/taxonomy to [redacted] with the detailed information necessary for tracking and reporting.

iv. The CPSC drafted an ERM framework guiding document and an operational risk profile that includes an identified IT risk. However, the ERM framework document is not adequately formalized and states that the CPSC is operating at an [']Ad Hoc[’] stage or level one maturity." Further, 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, and
   - The technology utilized to support the CPSC's information security program.

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

vi. The CPSC has not defined the roles and responsibilities of internal and external stakeholders involved in its risk management processes in support of a holistic information security risk management program that also supports the agency's Enterprise Risk Management Program.

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

Recommendations

We recommend that the CPSC:

1. Develop and implement a process to maintain an up-to-date and complete information system inventory (Risk Management.i) *(2020 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.ii/iii) *(prior year recommendation).*
3. Establish and implement a policy and procedures to manage software licenses using automated monitoring and expiration notifications (Risk Management.ii/iii) *(prior year recommendation).*
4. [redacted] *(prior year recommendation).*
5. Define and document the taxonomy of CPSC's information system components, and classify each information system component as, at minimum, one of the following types: IT 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 CPSC's operational mission, facility, or social media) (Risk Management.ii/iii) *(prior year recommendation).*
6. Identify and [redacted] that establishes set policies for hardware and software access on the agency's network (Risk Management.ii/iii) *(prior year 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.iv/v/vi) *(prior year recommendation – modified).*
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.iv/v/vi) *(prior year recommendation – modified).*
9. Develop and implement an Enterprise Risk Management (ERM) program based on National Institute of Standards and Technology and ERM Playbook (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.iv/v/vi) *(prior year recommendation).*
10. Develop and implement a supply chain risk management plan (Risk Management.iv/v/vi) *(prior year recommendation).*

11. Develop and implement an information security architecture that supports the CPSC Enterprise Architecture and is integrated into the agency's Enterprise Risk Management Program. (Risk Management.vii) *(2020 recommendation).*
12. Develop an Enterprise Architecture to be integrated into the risk management process *(prior year recommendation).*
13. Establish and implement policies and procedures to require coordination between the Office of Information Technology and the Office of Procurement to facilitate identification and incorporation of the appropriate clauses within all contracts *(prior year recommendation).*

4.2 Configuration Management

Conditions

In FY 2020, the CPSC made progress in addressing previously identified configuration management deficiencies. For example, the CPSC implemented new technologies and implemented several operating system updates on the CPSC network. However, based on evaluation procedures performed, Williams Adley identified the following deficiencies within the Configuration Management IG FISMA metric domain:

i. The CPSC has not developed a Change Control Board Charter.
ii. The CPSC has not established an Enterprise-wide Configuration Management Plan.
iii. The CPSC has not [redacted] under configuration control. In addition, the system components are not inventoried at a level of granularity deemed necessary for tracking and reporting.
iv. The CPSC has not developed procedures:
    - To ensure that [redacted] are defined, implemented, and monitored,
    - For documenting and managing deviations, and
    - That include clearly defined requirements for documenting testing results for its implemented system change requests.
v. [redacted].

Recommendations

We recommend that the CPSC:

14. Further define the resource designations for a Change Control Board (Configuration Management.i) *(prior year recommendation).*
15. Develop and implement a Configuration Management plan to ensure it includes all requisite information (Configuration Management.ii) *(prior year*

recommendation).

16. Develop, implement, and disseminate a set of Configuration Management (CM) procedures in accordance with the inherited CM Policy [redacted] (Configuration Management.iii/iv) *(prior year recommendation).*
17. Integrate the management of secure configurations into the organizational Configuration Management process (Configuration Management.iii/iv) *(prior year recommendation).*
18. Identify and document the characteristics of items that are to be placed under Configuration Management control (Configuration Management.v) *(prior year recommendation).*
19. Establish measures to evaluate the implementation of changes in accordance with documented information system baselines and integrated secure configurations (Configuration Management.v) *(prior year recommendation).*
20. Consistently implement [redacted], including the remediation of [redacted] (Configuration Management.v) *(2020 recommendation).*
21. Define and document all the critical capabilities that the CPSC manages internally as part of the Trusted Internet Connection (TIC) program *(prior year recommendation)*.

4.3 Identity and Access Management

Conditions

In FY 2020, the CPSC made progress in addressing previously identified identity and access management deficiencies. For example, the CPSC began implementing the tool CyberArk to assist with privileged user account management. However, based on evaluation procedures performed, Williams Adley identified the following deficiencies within the Identity and Access Management IG FISMA metric domain:

i. The CPSC has not developed an Identity, Credential, and Access Management (ICAM) strategy with roles, responsibilities, and stakeholders defined.
ii. The CPSC has not defined the following procedures for their ICAM program:
   - Account management processes for both privileged and non-privileged users,
   - [redacted], and
   - Identification and authentication management.
iii. The CPSC has not developed an ICAM strategy that includes a review of current practices, identification of gaps, and a transition plan.
iv. CPSC has not finalized Directives System Order 0311 (*Policies and Procedures Governing the Personnel Security and Suitability Program of the Consumer Product Safety Commission (CPSC)*) that governs its processes for assigning

personnel risk designations and performing appropriate screening prior to granting access to its information systems.

v. The CPSC has not defined its processes for ensuring the completion of required access agreement documentation (e.g. Rules of Behavior) for individuals that access its systems.

vi. The CPSC has not fully implemented required Personal Identity Verification authentication mechanisms for nonprivileged users of the CPSC's facilities and networks, including for remote access, in accordance with federal targets and directives as a result of current logistic challenges created by the ongoing pandemic. Although, the CPSC has implemented multi-factor authentication controls as a compensating control.

vii. The CPSC has not defined its processes for provisioning, managing, and reviewing [redacted].

Recommendations

We recommend that the CPSC:

22. Define and document a strategy (including specific milestones) to implement Federal Identity, Credential, and Access Management (Identity and Access Management.i-iii) *(prior year recommendation).*
23. Integrate the Identity, Credential, and Access Management strategy and activities into the Enterprise Architecture and Information Security Continuous Monitoring (Identity and Access Management.i-iii) *(prior year recommendation).*
24. Develop, formalize (through the CPSC's D-100 process), and implement processes to ensure all personnel are assigned risk designations and appropriately screened prior to being granted access to agency systems. Prior to formalizing the existing risk designation procedures, these procedures should be enhanced to include the following requirements:
    - Performance of periodic reviews of risk designations at least annually,
    - Explicit position screening criteria for information security role appointments,
    - Description of how cybersecurity is integrated into human resources practices (Identity and Access Management.iv) *(prior year recommendation).*
25. Develop and implement a process to ensure the completion of access agreements for all CPSC information system users (Identity and Access Management.v) *(2020 recommendation).*
26. Enforce Personal Identity Verification card usage for authenticating to all CPSC systems (Identity and Access Management.vi) *(prior year recommendation).*
27. Identify and document potentially incompatible duties permitted by [redacted] (Identity and Access Management.vii) *(prior year recommendation).*
28. [redacted] (Identity and Access Management.vii) *(prior year recommendation).*

29. Fully deploy the CPSC's [redacted] (Identity and Access Management.vii) *(prior year recommendation).*
30. [redacted] (Identity and Access Management.vii) *(prior year recommendation).*
31. Define and implement the identification and authentication policies and procedures (Identity and Access Management.vii) *(prior year recommendation).*
32. Automatically revoke temporary and emergency access after a specified period of time (Identity and Access Management.vii) *(prior year recommendation).*

4.4 Data Protection and Privacy

Conditions

In FY 2020, the CPSC made progress in addressing previously identified data protection and privacy deficiencies. For example, CPSC hired a full-time employee to serve as a Privacy Officer. However, based on evaluation procedures performed, Williams Adley identified the following deficiencies within the Data Protection and Privacy IG FISMA metric domain:

i. The CPSC has not developed a process for maintaining and tracking a PII inventory (the types of PII records maintained by system and their sources).
ii. The CPSC has not developed policies and procedures for encryption of data at rest and encryption of data in transit, in accordance with NIST or best practice guidance.
iii. The CPSC has not developed role-based privacy awareness training for all applicable personnel. Specifically, the CPSC has defined privacy training in the CPSC Privacy Program Plan, however, the CPSC has not defined requirements for role-based privacy awareness training and no role-based trainings have been provided to date.

Recommendations

We recommend that the CPSC:

33. 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 and Privacy.i) *(prior year recommendation).*
34. Document and implement a process for periodically reviewing for and removing unnecessary Personally Identifiable Information from agency systems (Data Protection and Privacy.i) *(prior year recommendation).*
35. Develop and implement data encryption policies and procedures (Data Protection and Privacy.ii) *(2020 recommendation).*
36. [redacted]

[redacted] *(prior year recommendation).*

4.5 Security Training

Conditions

In FY 2020, the CPSC made progress in addressing previously identified security training deficiencies. For example, the CPSC was able to complete prescribed annual security trainings and began revamping its role-based training processes. However, based on evaluation procedures performed, 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.
ii. The CPSC has not developed a security training plan or strategy that documents the funding for the security training program and overall goals.
iii. The CPSC has not fully implemented a role-based security and privacy training program in accordance with the CPSC's Role-based Training Knowledge, Skills, and Abilities document. In addition, the CPSC has not defined its processes for ensuring that all personnel with significant security roles and responsibilities are provided specialized security training prior to information system access or performing assigned duties and periodically thereafter. The CPSC has developed secure email, remote access, mobile devices, social media, phishing, physical security and incident reporting training material; however, the CPSC has not defined a process for measuring the effectiveness of its security awareness training.
iv. The CPSC has not defined its security training material based on its organizational requirements, culture, and the types of roles with significant security responsibilities.

Recommendations

We recommend that the CPSC:

37. Perform an assessment of the knowledge, skills, and abilities of CPSC personnel with significant security responsibilities (Security Training.i) *(prior year recommendation).*
38. Identify all CPSC personnel that affect security and privacy (e.g., Executive Risk Council, Freedom of Information Act personnel, etc.) and ensure the training policies are modified to require these individuals to participate in role-based security/privacy training (Security Training.ii) *(prior year recommendation).*
39. Develop and tailor security training content for all CPSC personnel with significant security responsibilities, and provide this training to the appropriate individuals (Security Training.iv) *(prior year recommendation)*

4.6 Information Security Continuous Monitoring

Conditions

In FY 2020, the CPSC made progress in addressing previously identified ISCM deficiencies. For example, the CPSC began planning for the assessment of program management and privacy controls. However, based on evaluation procedures performed, Williams Adley identified the following deficiencies within the ISCM IG FISMA metric domain:

i. The CPSC has implemented its ISCM program activities at the system level via annual control assessments. However, 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. The CPSC has not developed ISCM procedures that explicitly support its ISCM Plan. Specifically, analyzing ISCM data or performance measures that support its risk management program, reporting findings, and reviewing and updating the ISCM strategy.
iii. The CPSC has not developed ISCM program performance measures/metrics. For example, CPSC needs to define metrics to be used to evaluate and control ongoing risk to the CPSC within defined risk tolerance levels.

Recommendations

We recommend that the CPSC:

40. Integrate the established strategy for identifying organizational risk tolerance

into the Information System Continuous Monitoring plan (Information System Continuous Monitoring.i) *(prior year recommendation).*

41. Define and implement Information System Continuous Monitoring (ISCM) procedures, to include the monitoring of performance measures, that support updates to the ISCM plan (Information System Continuous Monitoring.ii) *(2020 recommendation).*

4.7 Incident Response

Conditions

In FY 2020, the CPSC made progress in addressing previously identified incident response deficiencies and continued to improve a well implemented program. For example, the CPSC developed technical standard operating procedures and consignment strategies for the various types of information security incidents faced. The CPSC also began using [redacted] as an intrusion detection tool. Further, the CPSC has also implemented techniques and technologies that aid them in profiling network activity, and in doing so, have vastly improved their ability to quickly identify potential indicators of compromise allowing for quicker and more targeted incident response. However, based on evaluation procedures performed, Williams Adley identified the following deficiencies within the Incident Response IG FISMA metric domain:

i. The CPSC has not updated and maintained its Incident Response Policy and Incident Response Plan in accordance with defined requirements.
ii. Based on received documentation, the CPSC has also not yet implemented explicit performance measures (outside incident response timing metrics) to evaluate the effectiveness of its incident response program and related activities.
iii. Although the CPSC does report potential incidents, the CPSC has not implemented an effective mechanism to evidence timely reporting to the United States Computer Emergency Readiness Team in accordance with new requirements.

Recommendations

We recommend that the CPSC:

42. Update and implement the CPSC Incident Response (IR) Policy and IR Plan with latest practices, including IR performance measures and the latest implemented network profiling techniques (Incident Response.i/ii) *(2020 recommendation).*
43. Define and implement a process to ensure the timely resolution of incidents. For example, establish routine status reviews for tracking incident response activities to completeness (Incident Response.iii) *(prior year recommendation).*

4.8 Contingency Planning

Conditions

In FY 2020, the CPSC made progress in addressing previously identified contingency planning deficiencies. For example, the CPSC was able to complete a business impact assessment for the General Support System and complete some system level contingency plan testing. However, based on evaluation procedures performed, Williams Adley identified the following deficiencies within the Contingency Planning IG FISMA metric domain:

i. The CPSC has not developed a complete set of contingency plans that included an organization-wide Continuity of Operations Plan and related Business Continuity Plans. The CPSC also has not yet defined supporting contingency planning procedures or an approach for supply chain risk management.
ii. The CPSC has completed surveying some of the CPSC program offices to aid them in identifying critical systems while completing the General Support System Business Impact Assessment (BIA). However, the BIA does not define the CPSC's Mission Essential Functions. Further, as stated within the BIA, some recovery timing requirements may not be enough for at least two program office major applications. In addition, the CPSC has not developed the other contingency planning documents required to support the BIA and a full Continuity of Operations Plan, such as a Disaster Recovery Plan (DRP).
iii. The CPSC has not developed their approach for how contingency planning integrates with other information security domains or requirements, especially risk management. For example, the CPSC has not defined a DRP, and instead has accepted the risk of not having a DRP developed. However, it is not clear that this risk acceptance is in line with CPSC's risk tolerance since the risk tolerance is not formally defined to guide the information security decisions. Further, although the CPSC has established an alternate storage site, the CPSC has not established an alternate processing site in accordance with the CPSC policy requirements, instead the CPSC is waiting to utilize potential cloud solutions.
iv. The CPSC has made updates to major systems information security contingency plans and completed tabletop exercises. However, the CPSC has not defined clear required testing procedures and did not integrate testing with other contingency plans.

Recommendations

We recommend that the CPSC:

44. Develop and document a robust and formal approach to contingency planning for agency systems and processes using the appropriate guidance [ex. National Institute of Standards and Technology (NIST) Special Publication 800-34/53, Federal Continuity Directive 1, NIST Cybersecurity Framework,

and National Archive and Records Administration guidance] (Contingency Planning.i) *(prior year recommendation).*

45. 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, and Information System Contingency Plans) in accordance with appropriate federal and best practice guidance (Contingency Planning.ii) *(prior year recommendation).*
46. Integrate documented contingency plans with the other relevant agency planning areas (Contingency Planning.iii) *(prior year recommendation).*
47. Test the set of documented contingency plans (Contingency Planning.iv) *(prior year recommendation).*

5. CONSOLIDATED LIST OF RECOMMENDATIONS

Table 5-1: Index of Recommendations

Finding	Recommendation
Risk Management	1. Develop and implement a process to maintain an up-to-date and complete information system inventory (*2020 recommendation*). 2. Develop, document, and implement a process for determining and defining system boundaries in accordance with National Institute of Standards and Technology guidance (*prior year recommendation*). 3. Establish and implement a policy and procedures to manage software licenses using automated monitoring and expiration notifications (*prior year recommendation*). 4. [redacted] (*prior year recommendation*). 5. Define and document the taxonomy of CPSC's information system components, and classify each information system component as, at minimum, one of the following types: IT 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 CPSC's operational mission, facility, or social media) (*prior year recommendation*). 6. Identify and [redacted] that establishes set policies for hardware and software access on the agency's network (*prior year 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 (*prior year recommendation - modified*). 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 (*prior year recommendation - modified*). 9. Develop and implement an Enterprise Risk Management (ERM) program based on National Institute of Standards and Technology and ERM Playbook (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 (*prior year recommendation*). 10. Develop and implement a supply chain risk management plan (*prior year recommendation*). 11. Develop and implement an information security architecture that supports the CPSC Enterprise Architecture and is integrated into the agency's Enterprise Risk Management Program (*2020 recommendation*).

	12. Develop an Enterprise Architecture to be integrated into the risk management process (*prior year recommendation*). 13. Establish and implement policies and procedures to require coordination between the Office of Information Technology and the Office of Procurement to facilitate identification and incorporation of the appropriate clauses within all contracts (*prior year recommendation*).
Configuration Management	14. Further define the resource designations for a Change Control Board *(prior year recommendation).* 15. Develop and implement a Configuration Management plan to ensure it includes all requisite information *(prior year recommendation).* 16. Develop, implement, and disseminate a set of Configuration Management (CM) procedures in accordance with the inherited CM Policy [redacted] *(prior year recommendation).* 17. [redacted] *(prior year recommendation).* 18. Identify and document the characteristics of items that are to be placed under Configuration Management control *(prior year recommendation).* 19. Establish measures to evaluate the implementation of changes in accordance with documented information system baselines and integrated secure configurations *(prior year recommendation).* 20. Consistently implement [redacted], including the remediation of [redacted] (*2020 recommendation).* 21. Define and document all the critical capabilities that the CPSC manages internally as part of the Trusted Internet Connection (TIC) program *(prior year recommendation)*.
Identity and Access Management	22. Define and document a strategy (including specific milestones) to implement Federal Identity, Credential, and Access Management *(prior year recommendation).* 23. Integrate Identity, Credential, and Access Management strategy and activities into the Enterprise Architecture and Information System Continuous Monitoring *(prior year recommendation).* 24. Develop, formalize (through the CPSC's D-100 process), and implement processes to ensure all personnel are assigned risk designations and appropriately screened prior to being granted access to agency systems. Prior to formalizing the existing risk designation procedures, these procedures should be enhanced to include the following requirements: • Performance of periodic reviews of risk designations at least annually, • Explicit position screening criteria for information security role appointments, • Description of how cybersecurity is integrated into human resources practices *(prior year recommendation).*

	25. Develop and implement a process to ensure the completion of access agreements for all CPSC information system users *(2020 recommendation).* 26. Enforce Personal Identity Verification card usage for authenticating to all CPSC systems *(prior year recommendation).* 27. Identify and document potentially incompatible duties permitted by [redacted] *(prior year recommendation).* 28. [redacted] *(prior year recommendation).* 29. Fully deploy the CPSC's [redacted] *(prior year recommendation).* 30. [redacted] *(prior year recommendation).* 31. Define and implement the identification and authentication policies and procedures *(prior year recommendation).* 32. Automatically revoke temporary and emergency access after a specified period of time *(prior year recommendation).*
Data Protection and Privacy	33. Document and implement a process for inventorying and securing systems that contain Personally Identifiable Information or other sensitive agency data (e.g., proprietary information) *(prior year recommendation).* 34. Document and implement a process for periodically reviewing for and removing unnecessary Personally Identifiable Information from agency systems *(prior year recommendation.)* 35. Develop and implement data encryption policies and procedures *(2020 recommendation).* 36. [redacted] *(prior year recommendation).*
Security Training	37. Perform an assessment of the knowledge, skills, and abilities of CPSC personnel with significant security responsibilities *(prior year recommendation).* 38. Identify all CPSC personnel that affect security and privacy (e.g., Executive Risk Council, Freedom of Information Act personnel, etc.) and ensure the training policies are modified to require these individuals to participate in role-based security/privacy training *(prior year recommendation).* 39. Develop and tailor security training content for all CPSC personnel with significant security responsibilities, and provide this training to the appropriate individuals *(prior year recommendation).*
Information Security Continuous Monitoring	40. Integrate the established strategy for identifying organizational risk tolerance into the Information System Continuous Monitoring plan *(prior year recommendation).* 41. Define and implement Information System Configuration Management (ISCM) procedures, to include the monitoring of

	performance measures, that support the updates ISCM plan *(2020 recommendation).*
Incident Response	42. Update and implement the CPSC Incident Response (IR) policy and IR plan with latest practices, including IR performance measurers and the latest implemented network profiling techniques *(2020 recommendation).* 43. Define and implement a process to ensure the timely resolution of incidents. For example, establish routine status reviews for tracking incident response activities to completeness *(prior year recommendation).*
Contingency Planning	44. Develop and document a robust and formal approach to contingency planning for agency systems and processes using the appropriate guidance [ex. National Institute of Standards and Technology (NIST) Special Publication 800-34/53, Federal Continuity Directive 1, NIST Cybersecurity Framework, and National Archive and Records Administration guidance] *(prior year recommendation).* 45. 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, and Information System Contingency Plans) in accordance with appropriate federal and best practice guidance *(prior year recommendation).* 46. Integrate documented contingency plans with the other relevant agency planning areas *(prior year recommendation).* 47. Test the set of documented contingency plans *(prior year 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[9] for FY 2020. In support of this objective, Williams Adley conducted the evaluation in accordance with OMB 20-04, *FY 2019 - 2020 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 2020. 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 for the evaluation:

- General Support System (Local Area Network)
- Consumer Product Safety Risk Management System
- CPSC Public Website (CPSC.gov)
- Dynamic Case Management
- International Trade Data System/Risk Automation Methodology System

A.3 Methodology

Williams Adley 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 2020 IG FISMA Reporting Metrics:

- Identify (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

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

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 inspector to perform annual reviews of the information security program and that the head of the agency report those results to OMB. The FY 2020 IG FISMA Reporting Metrics developed by the OMB, DHS, and Council of Inspectors General on Integrity and Efficiency (CIGIE) is intended to provide guidance on the OIG's annual evaluations, as required by the FISMA, 44 U.S. Code, section 3555(j).

Williams Adley performed this evaluation from April through September 2020 and conducted this evaluation in accordance with CIGIE Quality Standards for Evaluation and Inspection. Those standards require that Williams Adley obtains sufficient evidence to provide a reasonable basis for Williams Adley's findings and conclusions based on Williams Adley's evaluation objectives.

To perform this evaluation, Williams Adley interviewed the CPSC senior management and employees to evaluate managerial effectiveness and operational controls in accordance with NIST and OMB guidance. Williams Adley 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 written documents to supplement observations and interviews. Williams Adley provided a draft report to the management on October 19, 2020 and an exit conference was held on October 20, 2020, to discuss the results of the evaluation.

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 that CPSC personnel obtain system generated reports of the information system inventory. These reports were used to support the evaluation procedures in the risk management 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 the 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

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.[10] This guidance assists in applying sampling in accordance with auditing standards.

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 judgement of risk. 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 accordance with guidance from the following:

- Chief Financial Officers Council, Enterprise Risk Management Playbook
- Chief Information Officer Council/Chief Acquisition Officer Council, Cloud Computing Contract Best Practices
- Council of Inspectors General on Integrity and Efficiency, Quality Standards for Inspection and Evaluation
- Cybersecurity Sprint
- Cybersecurity Strategy and Implementation Plan
- Department of Homeland Security Binding Operational Directive 15-01
- Department of Homeland Security Binding Operational Directive 17-01
- Department of Homeland Security Cyber Incident Reporting Unified Message
- E-Government Act of 2002
- Federal Acquisition Regulation sections 39.101, 105, 52.224-1, 52.224-2, and 52.239-1
- Federal Continuity Directive 1
- Federal Cybersecurity Workforce Assessment Act of 2015
- Federal Enterprise Architecture Framework
- Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance

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

- Federal Information Processing Standards 199
- Federal Information Processing Standards 201-2
- Federal Information Security Modernization Act of 2014
- Federal Risk and Authorization Management Program - Standard Contract Clauses
- FY 2020 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics
- Homeland Security Presidential Directive 12
- Government Accountability Office, *Standards for Internal Control in the Federal Government*
- National Archives and Records Administration, *Guidance on Information Systems Security Records*
- National Cybersecurity Workforce Framework
- National Insider Threat Policy
- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- National Institute of Standards and Technology (NIST) SP 800-30
- National Institute of Standards and Technology (NIST) SP 800-34
- National Institute of Standards and Technology (NIST) SP 800-37, Revision (Rev) 2
- National Institute of Standards and Technology (NIST) SP 800-39
- National Institute of Standards and Technology (NIST) SP 800-40, Rev 3
- National Institute of Standards and Technology (NIST) SP 800-44
- National Institute of Standards and Technology (NIST) SP 800-50
- National Institute of Standards and Technology (NIST) SP 800-53, Rev 4
- National Institute of Standards and Technology (NIST) SP 800-60
- National Institute of Standards and Technology (NIST) SP 800-61, Rev 2
- National Institute of Standards and Technology (NIST) SP 800-63
- National Institute of Standards and Technology (NIST) SP 800-83
- National Institute of Standards and Technology (NIST) SP 800-84
- National Institute of Standards and Technology (NIST) SP 800-86
- National Institute of Standards and Technology (NIST) SP 800-122
- National Institute of Standards and Technology (NIST) SP 800-128
- National Institute of Standards and Technology (NIST) SP 800-137
- National Institute of Standards and Technology (NIST) SP 800-161
- National Institute of Standards and Technology (NIST) SP 800-181
- National Institute of Standards and Technology (NIST) SP 800-184
- Office of Management and Budget (OMB) Circular No. A-11
- Office of Management and Budget (OMB) Circular No. A-123
- Office of Management and Budget (OMB) Circular No. A-130, Appendix I
- Office of Management and Budget (OMB) Memorandum 04-25
- Office of Management and Budget (OMB) Memorandum 08-05
- Office of Management and Budget (OMB) Memorandum 14-03

- Office of Management and Budget (OMB) Memorandum 14-04
- Office of Management and Budget (OMB) Memorandum 16-03
- Office of Management and Budget (OMB) Memorandum 16-04
- Office of Management and Budget (OMB) Memorandum 16-17
- Office of Management and Budget (OMB) Memorandum 17-09
- Office of Management and Budget (OMB) Memorandum 17-12
- Office of Management and Budget (OMB) Memorandum 17-25
- Office of Management and Budget (OMB) Memorandum 18-02
- Office of Management and Budget (OMB) Memorandum 19-02
- Office of Management and Budget (OMB) Memorandum 20-04
- Presidential Policy Directive (PPD) - 41
- Privacy Act of 1974
- SANS Institute, *Critical Security Controls*
- Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*
- Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*
- US-Computer Emergency Readiness Team, *Federal Incident Notification & Response Guidelines*
- US-Computer Emergency Readiness Team, *Incident Notification Guidelines*
- US-Computer Emergency Readiness Team, *Incident Response Guidelines*

Appendix B. Management Response

In response to the Fiscal Year 2020 Federal Information Security Modernization Act of 2014 (FISMA) Evaluation, Management generally concurs with the report's findings and recommendations and acknowledges that many of those findings and recommendations are important to the protection of agency systems and information.

We acknowledge deficiencies in areas identified in the report, but at the same time, staff states that there are existing program functions that are substantially effective, and that the identified deficiencies do not undermine the overall CPSC information security program. Staff points to the following accomplishments in FY20 to underscore steps it has taken to advance information security at CPSC:

- Performed timely independent security assessments of all major information systems and the agency's general support system (GSS);
- Implemented system hardware, software, and network connectivity required to integrate the agency's systems into the DHS Continuous Diagnostics and Mitigation (CDM) program;
- Significantly increased the use of data analysis tools to perform real-time capturing, indexing, and correlating of network security data to produce graphs, actionable alerts, dashboards, and visualizations—which help to greatly improve overall awareness of the agency's system security posture;
- Deployed an [redacted] tool to help identify and contain malicious activity on agency systems;
- Deployed data loss protection (DLP) capability to scan and block outgoing agency email containing Social Security Numbers;
- Implemented enhancements to agency Plan of Action and Milestones (POAM) processes, which resulted in a 22% decrease in open POAMs across all major agency systems;
- Defined and implemented file sharing/cloud storage security controls to help prevent undisclosed data transfers to unauthorized cloud storage sites;
- Conducted a risk and vulnerability assessment in coordination with the Department of Homeland Security (DHS), which led to improvements in both internal and external system security controls.

Additionally, current effective operational practices include the following baseline security controls:

- The agency's hardware assets are covered by an enterprise-level automatic hardware asset inventory capability;
- The agency's critical systems have active security Authorizations to Operate (ATO) and System Security Plans (SSP);
- Remote connections to agency systems employ National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2 validated cryptographic modules;
- All standard network users are required to log onto the network with a [redacted];
- The agency's physical access control systems electronically accept and authenticate PIV credentials for physical access to agency offices;
- The agency's systems are scanned regularly for vulnerabilities using

[redacted] tools;
• All government furnished endpoints and mobile devices encrypt data at rest;
• The agency's users are tested regularly on their understanding and recognition of phishing threats using simulated phishing exercises;
• The agency has fully implemented [redacted] tools to detect and block attacks and provide insights to [redacted] to support government-wide situational awareness.
• The agency provided role-based security training to all employees with significant security responsibilities—to include system administrators, application developers, database administrators, auditors, and privacy personnel.

Management believes that the number of deficiencies in the FY 2020 FISMA evaluation requires staff to appropriately prioritize recommendations so that, given limited agency resources, the most significant risks to agency systems and information are addressed first. We believe this approach would improve the agency's overall security posture, and, at the same time, provide the most efficient use of agency resources. Accordingly, although we will seek to address all of the recommendations to the extent feasible and within available resources, we will prioritize the following recommendations for remediation:

1. Consistently implement [redacted], including the remediation of critical vulnerabilities.
2. Identify and implement a [redacted] solution that establishes set policies for hardware and software access on the agency's network.
3. Develop and implement a CM plan to ensure it includes all requisite information.
4. Develop, implement, and disseminate a set of CM procedures in accordance with the inherited CM Policy which includes the process management follows to develop and tailor common secure configurations (hardening guides) and to approve deviations from those standard configurations.
5. Document and implement a process to restrict the use of [redacted] when performing [redacted].
6. Fully deploy the CPSC's [redacted] solution.
7. Develop and implement data [redacted] policies and procedures.

Management notes that it has requested additional funding in agency budget requests to assist in remediating audit findings. Finally, although we generally concur with the audit findings, staff provides the following information for purposes of providing additional clarity on the following specific finding in the report:

The [redacted] of the CPSC's facilities and networks, including for [redacted], in accordance with federal targets and directives as a result of current

logistic challenges created by the ongoing pandemic. Although CPSC has implemented [redacted] as a compensating control.

The agency has fully implemented required [redacted] as the standard authentication mechanism for access to the agency's network—including remote access. The agency, in accordance with OMB Memorandum M-20-19, issued [redacted] to accommodate employees whose [redacted] due to limits on building access as a result of the current pandemic. The agency also provides [redacted] as a temporary access mechanism for employees who lose or misplace a [redacted]. Staff believes these measures are sufficient and appropriate and that a total [redacted] requirement would result in a significant disruption of agency operations and services.

Mary Boyle

Mary Boyle, Executive Director

Appendix C. Acronyms

BIA	Business Impact Assessment
CIGIE	Council of Inspectors General on Integrity and Efficiency
CM	Configuration Management
CPSC	U.S. Consumer Product Safety Commission
Cybersecurity Framework	Framework for Improving Critical Infrastructure Cybersecurity
DHS	Department of Homeland Security
DRP	Disaster Recovery Plan
ERM	Enterprise Risk Management
EXIT	Office of Information and Technology Services
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
ICAM	Identity, Credential, and Access Management
IG	Inspector General
IR	Incident Response
ISCM	Information System Continuous Monitoring
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
Rev	Revision
SP	Special Publication
Williams Adley	Williams, Adley, & Co.-DC LLP

CONTACT US

If you want to confidentially report or discuss any instance of fraud, waste, abuse, misconduct, or mismanagement involving CPSC's programs and operations, please contact the CPSC Office of Inspector General.

Call:

301-504-7906
1-866-230-6229

On-line complaint form:

Click here for complaint form.
Click here for CPSC OIG Website.

Write:

Office of Inspector General
Consumer Product Safety Commission
4330 East-West Highway, Room 702
Bethesda MD 20814