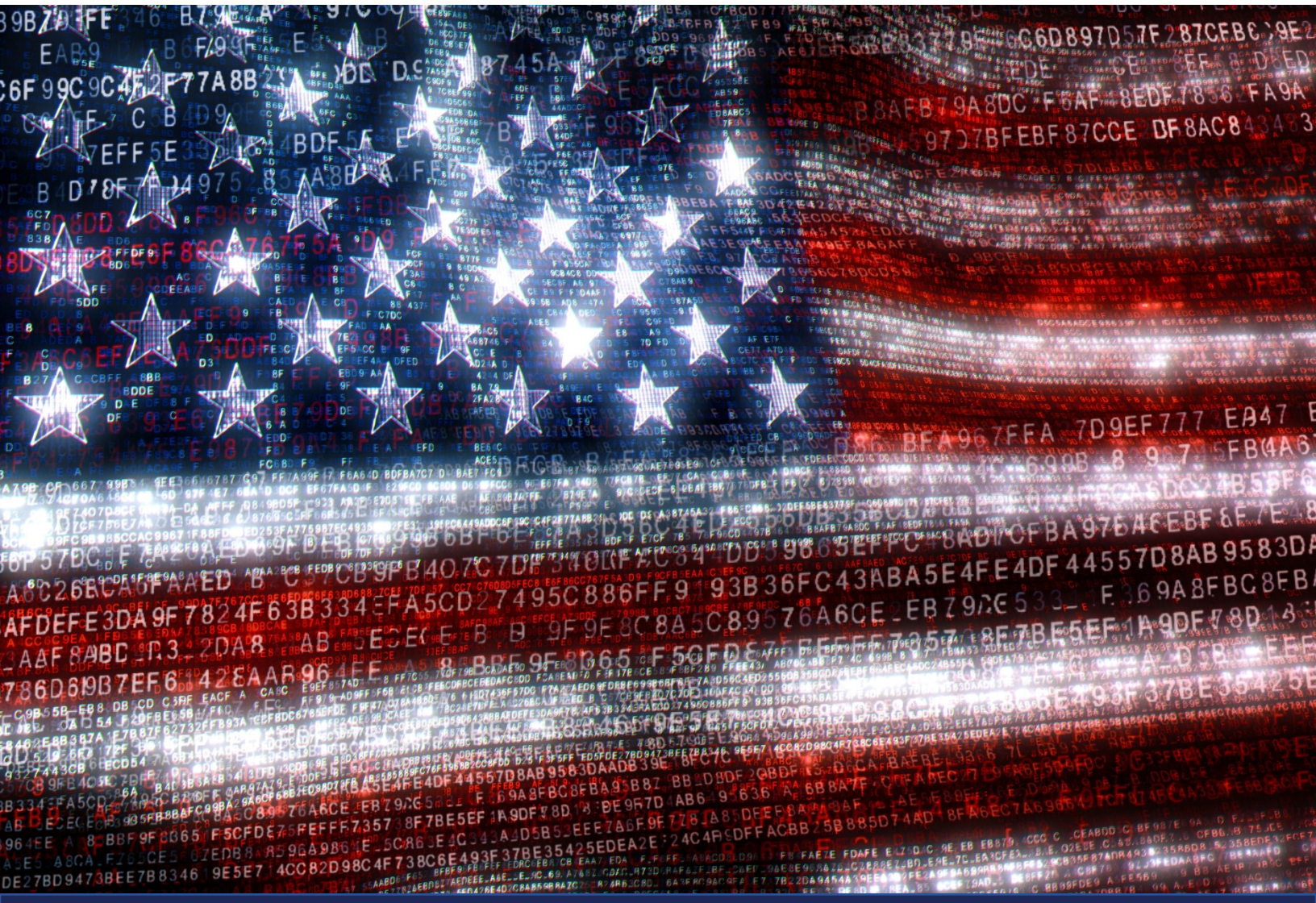
U.S. Consumer Product Safety Commission
OFFICE OF INSPECTOR GENERAL



Evaluation of the CPSC's FISMA Implementation for FY 2021

October 29, 2021

22-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.

October 29, 2021

TO: Alexander Hoehn-Saric, Chairman
Robert S. Adler, Commissioner
Dana Baiocco, Commissioner
Peter A. Feldman, Commissioner

FROM: Christopher W. Dentel, Inspector General CHRISTOPHER DENTEL Digitally signed by CHRISTOPHER DENTEL Date: 2021.10.28 05:38:30 -04'00'

SUBJECT: Evaluation of the CPSC's FISMA Implementation for FY 2021

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 2021, 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. 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. 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. This is a step the CPSC has repeatedly failed to take.

This year's FISMA report contains 47 recommendations. The CPSC closed 5 of the recommendations from last year, 5 new recommendations were made, and 42 recommendations were repeated from last year. 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. 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.

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) 2021 and to determine the effectiveness of its information security program. This report documents the results of the FISMA evaluation. Specifically, we 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 made progress in implementing FISMA requirements. Specifically, the CPSC closed five recommendations included in the FY 2020 FISMA report and completed the following activities:

- Implemented a new tool to identify deviations from common secure configurations.
- Began the final phases of implementing a privileged user account management tool.
- Developed procedures and implemented safeguards to prevent Domain Name Server (DNS) infrastructure tampering.
- Updated security training and role-based training procedures.
- Updated the Information Security Continuous Monitoring (ISCM) plan and defined system-level performance measures for configuration settings, vulnerability management, security impact analysis, and authorizations to operate.
- Defined and documented all the critical capabilities that the CPSC manages internally as part of the Trusted Internet Connection program.
- Transitioned to a new Security Information and Event Management (SIEM) tool for log aggregation analysis and alerting as well as to improve integration with the CPSC's other incident response tools.

- Completed testing the General Support System Local Area Network (GSS LAN) and International Trade Data System/Risk Assessment Methodology (ITDS/RAM) information system contingency plans (ISCPs).

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 FY 2020 FISMA evaluation. Instead, according to agency management, the CPSC focused its resources and effort on maintaining operational capability, transitioning a portion of its network to the Cloud, developing new and enhancing existing systems, and responding to an unprecedented number of government-wide critical security vulnerabilities and emergency directives from DHS, in addition to the resources and effort it spent on planning, managing budgets, and coordinating procurements. In order to achieve effective information security, the CPSC must prioritize the improvement of its information technology (IT) 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 audit 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 47 recommendations that the CPSC must address in order to mature its information security program. We provided 5 new recommendations and reissued 42 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 2021.

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 *21-02, Fiscal Year 2020-2021 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.

The CPSC OIG retained Williams Adley to perform an independent evaluation of the CPSC's implementation of FISMA for FY 2021. 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 for submission 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 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 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. As a result of the Executive Order, the National Institute of Standards and Technology (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 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 holds agency heads accountable for ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes.

The Cybersecurity Framework provides federal agencies with a common structure for identifying and managing information security risks across the enterprise and provides guidance for assessing the maturity of controls established to address those risks. The Cybersecurity Framework contains five information security functions that give federal agencies the ability to select and prioritize improvements in information security risk management. The five information security functions are as follows:

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

[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.

- **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 preceding it. For example, an organization cannot *protect* its IT 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 2021 Reporting Metrics

FISMA requires OMB to ensure that guidance is developed for the independent audit of agency information security programs. On May 12, 2021, the OMB, DHS, and the Council of Inspectors General on Integrity and Efficiency (CIGIE) released the *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.1*.

This guidance provides metrics to be used to gauge the maturity of agency practices in connection with the nine (9) IG FISMA metric domains that are organized around the five (5) information security functions outlined in the Cybersecurity Framework:

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

- **Respond**

  - *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.

- **Recover**

  - *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.

Key Changes to the FY 2021 IG FISMA Reporting Metrics

The FY 2021 FISMA reporting metrics included changes to 1) focus on increasing the maturity of the federal government's SCRM practices through the introduction of a new domain within the Identify function, SCRM, and 2) improve vulnerability identification, management, and remediation.

The new SCRM domain introduces five (5) metrics which focus on the maturity of agency SCRM strategies, policies and procedures, plans, and processes 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. The new domain references SCRM criteria in NIST Special Publication (SP) 800-53, Revision (Rev.) 5, *Security and Privacy Controls for Information Systems and Organizations,* released in September 2020 and updated in December 2020. To provide agencies with sufficient time to fully implement NIST SP 800-53, Rev. 5, in accordance with OMB Circular A-130, the SCRM domain will not be considered for the purposes of the Identify framework function rating.

On September 2, 2020, OMB released Memorandum 20-32, *Improving Vulnerability Identification, Management, and Remediation*, which provides guidance to federal agencies on collaborating with members of the public to find and report

vulnerabilities on federal information systems. On the same day, DHS published Binding Operational Directive 20-01, *Develop and Publish a Vulnerability Disclosure Policy*, which provides guidance on the development and publication of an agency's vulnerability disclosure policy and supporting vulnerability handling procedures. To address the new OMB Memorandum and DHS Binding Operational Directive, the IG FISMA Reporting Metrics introduced a new metric which focuses on determining whether agencies utilize a vulnerability disclosure policy as part of their vulnerability management program for internet-accessible federal systems.

NIST Risk Management Framework

NIST has established the information security risk management best practices via the risk management framework as detailed in the NIST SP 800-37, 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.

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 has five levels:

- **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 2021 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 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 2021 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 2021.

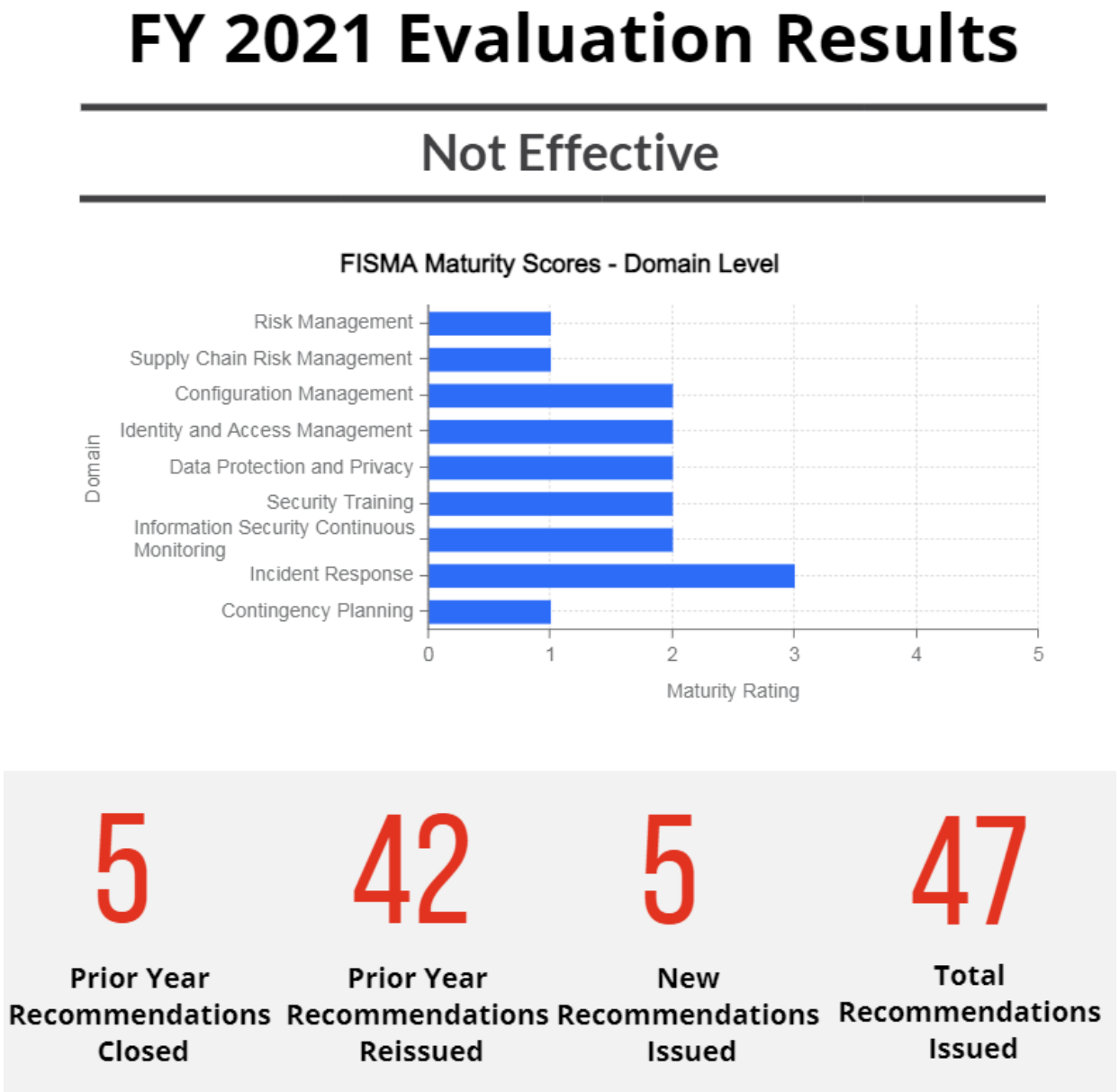


Figure 3-1. FY 2021 Evaluation Results

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 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. Although the CPSC has continued to develop an Enterprise Risk Management (ERM) program to guide its risk management practices, explicit guidance and processes to address information security risks and integrate those risks into the broader agency wide ERM program still have not been developed. The CPSC Office of Information Technology (EXIT) 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 EXIT has not received specific direction from the ERM program manager 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 FY 2020.

Furthermore, according to management, the CPSC focused its efforts in FY 2021 on IT operations and protecting, developing, and enhancing existing CPSC information systems, as well as implementing new solutions - including implementing two new Cloud solutions. Management also asserts that the CPSC spent considerable resources and effort on IT operations planning, managing budgets, coordinating procurements, and maintaining the CPSC networks.

CPSC personnel also noted that competing priorities continue to make it difficult to address previously identified information security program deficiencies while also meeting the demands of continuously emerging cybersecurity challenges. For example, management noted that there were numerous DHS cybersecurity directives issued throughout FY 2021 related to patching critical vulnerabilities. Meeting the DHS mandates was a priority for EXIT.

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 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 agency 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 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 each IG FISMA metric domain. Below we have provided a list of recommendations associated with each relevant condition in the corresponding section. A majority of the recommendations (42) identified below are directly related to prior year deficiencies and are prior year recommendations, while five (5) of the recommendations identified below are new this year as indicated by the parenthetical reference "(2021 recommendation)."

4.1 Identify Function Area

Progress

In FY 2021, the CPSC made progress in addressing previously identified risk management deficiencies. For example, the CPSC has started to implement a hardware inventory tracking application that gathers hardware information from computers and other devices on the agency's network for management, compliance, and audit purposes. Overall, the CPSC has made progress on open prior year recommendations, but not enough to close any findings.

Risk Management Conditions

In FY 2021, based on evaluation procedures performed, Williams Adley determined that the Risk Management IG FISMA metric domain was operating at the Maturity Level 1 - Ad-hoc. 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.

ii. The CPSC has not developed a process for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting.

iii. The CPSC has not developed a process for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses utilized in the organization's environment with the detailed information necessary for tracking and reporting.

iv. In FY 2020, the CPSC drafted an ERM framework guidance document and an operational risk profile that included an identified IT risk. However, the ERM framework document was not formalized, has not been updated since our last review, 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:

   a. scope and associated processes of the risk management strategy at each CPSC tier (e.g., at the enterprise, business process, and information system levels)
   b. roles and responsibilities of key personnel (including the risk executive function) or equivalent
   c. the CPSC information security risk profile, risk appetite, and risk tolerance, as applicable
   d. the CPSC's processes and methodologies for framing, assessing, categorizing, responding, addressing, and monitoring information security risks
   e. processes for communication of the risk management strategy across the CPSC
   f. the technology utilized to support the CPSC's information security program
   g. the development and use of a cybersecurity risk register or comparable mechanism

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

vi. The CPSC has not defined the roles and responsibilities of 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 ERM program.

vii. The CPSC developed an enterprise architecture target framework; however, 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.

Supply Chain Risk Management Conditions

The SCRM domain was added to the IG FISMA metrics in FY 2021. These metrics will not be used to evaluate the maturity of the agency's information security programs in FY 2021 in order to provide organizations with sufficient time to implement NIST SP 800-53, Rev. 5. Williams Adley determined that the Supply Risk Management IG FISMA metric domain was operating at the Maturity Level 1 - Ad-hoc. Williams Adley identified the following areas of improvement in preparation for the CPSC's implementation of NIST SP 800-53, Rev. 5 in FY 2022:

i. The CPSC has not defined and communicated an organization-wide SCRM plan or strategy.
ii. The CPSC has not defined and communicated its SCRM policies, procedures, and processes.
iii. 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.
iv. The CPSC has not defined and communicated its component authenticity policies and procedures.

Identify Function 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).*
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*).
3. Establish and implement policies and procedures to manage software licenses using automated monitoring and expiration notifications (*Risk Management ii/iii*).
4. Establish and implement a policy and procedure to ensure that only authorized hardware and software execute on the agency's network (*Risk Management ii/iii*).
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: 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 the CPSC's operational mission, facility, or social media) (*Risk Management ii/iii).*
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 ii/iii).*

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*).
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*).
9. Develop and implement an Enterprise Risk Management (ERM) program based on the National Institute of Standards and Technology and ERM Playbook (Office of Management and Budget 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 iv/v/vi*).
10. Develop and implement a supply chain risk management plan (*Supply Chain Risk Management i*).
11. Develop and implement an information security architecture that supports the Enterprise Architecture. (*Risk Management vii*).
12. Develop an Enterprise Architecture to be integrated into the risk management process *(Risk Management vii).*
13. Develop supply chain risk management policies and 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 ii/iii/iv*) (2021 recommendation).

4.2 Protect Function Area

Progress

The CPSC made progress in addressing previously identified Configuration Management deficiencies in FY 2021. For example, the CPSC implemented a new tool for identifying deviations from common secure configurations and defined and documented all of the critical capabilities that the CPSC manages internally as part of the Trusted Internet Connection program. Therefore, the CPSC was able to close one prior year recommendation.

The CPSC has also made progress in addressing previously identified Identity and Access Management deficiencies in FY 2021. For example, the CPSC is in the final phases of implementing a privileged access management solution. In addition, the CPSC was able to close one prior year recommendation by revoking temporary and emergency access automatically after a specified period of time.

Furthermore, the CPSC made progress in addressing previously identified Data Protection and Privacy deficiencies in FY2021. For example, the CPSC developed

procedures and implemented safeguards to prevent DNS infrastructure tampering and therefore was able to close one prior year recommendation.

Lastly, the CPSC made some progress in addressing previously identified security training deficiencies in FY 2021. For example, the CPSC security training and role-based training procedures were updated to reflect the CPSC's current training record management system. Overall, the CPSC has made progress on open prior year recommendations, but not enough to close any findings.

Configuration Management Conditions

Based on the evaluation procedures performed, Williams Adley determined that the Configuration Management IG FISMA metric domain was operating at the Maturity Level 2 - Defined. 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 finalized system-level Configuration Management Plan(s) for the GSS LAN and GSS Cloud.
iv. The CPSC has not drafted procedures to ensure that baseline configurations for its information systems are developed, documented, and maintained under configuration control. In addition, the system components are not inventoried at a level of granularity deemed necessary for tracking and reporting.
v. The CPSC has not developed procedures to:
    a. ensure that configuration settings/common secure configurations are defined, implemented, and monitored;
    b. document and manage deviations from authorized configuration settings/common secure configurations; and
    c. define requirements to document testing results for its implemented system change requests.
vi. The CPSC does not consistently implement its flaw remediation policies, procedures, and processes. The CPSC does not ensure that patches, hotfixes, service packs, and anti-virus/malware software updates are identified, prioritized, tested, and installed in a timely manner.
vii. The CPSC has not consistently implemented its configuration change control processes. Specifically, the CPSC does not consistently test changes prior to implementation.

Identity and Access Management Conditions

Based on the evaluation procedures performed, Williams Adley determined that the Identity and Access Management IG FISMA metric domain was operating at the Maturity Level 2 - Defined. 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:
    a. Account management processes for both privileged and non-privileged users
    b. Separation of duties and the Principle of Least Privilege
    c. 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. The 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, Personal Identity Verification (PIV) Acknowledgement form) for individuals that access its systems. Specifically, seven (7) out of seven (7) selected users did not complete the PIV acknowledgement form as required by Directive Order No. 0740.1, *Personnel Identity Credential*.
vi. The CPSC has not fully implemented required PIV 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 privileged accounts.

Data Protection and Privacy Conditions

Based on the evaluation procedures performed, Williams Adley determined that the Data Protection and Privacy IG FISMA metric domain was operating at the Maturity Level 2 - Defined. 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 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, while the CPSC has defined privacy training in the CPSC Privacy Program Plan, the CPSC has not defined requirements for

role-based privacy awareness training and no role-based trainings have been provided to date.

Security Training Conditions

Based on the evaluation procedures performed, Williams Adley determined that the Security Training IG FISMA metric domain was operating at the Maturity Level 2 - Defined. 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, 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.
iv. The CPSC has not defined a process for measuring the effectiveness of its security awareness training.
v. The CPSC has not defined its security training material based on its organizational requirements, culture, and the types of roles with significant security responsibilities.

Protect Function Recommendations

We recommend that the CPSC:

14. Further define the resource designations for a Change Control Board (*Configuration Management i*).
15. Develop and implement a Configuration Management plan to ensure it includes all requisite information (*Configuration Management ii/iii*).
16. Develop, implement, and disseminate a set of Configuration Management procedures in accordance with the inherited Configuration Management Policy which includes the process management follows to develop and tailor common secure configurations (hardening guides) and to approve deviations from those standard configurations (*Configuration Management iv/v*).
17. Integrate the management of secure configurations into the organizational Configuration Management process (*Configuration Management v*).
18. Consistently implement flaw remediation processes, including the remediation of critical vulnerabilities (*Configuration Management vi*).
19. Identify and document the characteristics of items that are to be placed under

Configuration Management control (*Configuration Management vii*).

20. Establish measures to evaluate the implementation of changes in accordance with documented information system baselines and integrated secure configurations (*Configuration Management vii*).
21. Define and document a strategy (including specific milestones) to implement the Federal Identity, Credential, and Access Management architecture (*Identity and Access Management i/ii/iii).*
22. Integrate Identity, Credential, and Access Management strategy and activities into the Enterprise Architecture and Information Security Continuous Monitoring (*Identity and Access Management i/ii/iii*).
23. 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*).
24. Define and implement a process to ensure the completion of access agreements for all CPSC users (*Identity and Access Management v*).
25. Enforce Personnel Identity Verification card usage for authenticating to all CPSC systems (*Identity and Access Management vi*).
26. Identify and document potentially incompatible duties permitted by privileged accounts (*Identity and Access Management vii*).
27. Document and implement a process to restrict the use of privileged accounts and services when performing non-privileged activities (*Identity and Access Management vii*).
28. Fully deploy the CPSC's privileged access management solution (*Identity and Access Management vii*).
29. Log and actively monitor activities performed while using privileged access that permit potentially incompatible duties (*Identity and Access Management vii*).
30. Define and implement the identification and authentication policies and procedures (*Identity and Access Management ii*).
31. Define and implement processes for provisioning, managing, and reviewing privileged accounts (*Identity and Access Management vii*) (2021 recommendation).
32. 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*).
33. Document and implement a process for periodically reviewing for and removing unnecessary Personally Identifiable Information from agency systems (*Data Protection and Privacy i).*
34. Develop and implement data encryption policies and procedures (*Data Protection*

and Privacy ii).

35. 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 (*Data Protection and Privacy iii*).
36. Perform an assessment of the knowledge, skills, and abilities of CPSC personnel with significant security responsibilities (*Security Training i*).
37. Document and implement a process for ensuring that all personnel with significant security roles and responsibilities are provided specialized security training to perform assigned duties (*Security Training ii/iii*) (2021 recommendation).
38. 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/v*).

4.3 Detect Function

Progress

In FY 2021, the CPSC made progress in addressing previously identified ISCM deficiencies. For example, the CPSC updated the ISCM plan and defined system-level performance measures for configuration settings, vulnerability management, security impact analysis, and authorizations to operate (ATO). Accordingly, the CPSC was able to close one prior year recommendation related to defining ISCM procedures for monitoring performance measures.

Information Security Continuous Monitoring Conditions

Based on the evaluation procedures performed, Williams Adley determined that the ISCM IG FISMA metric domain was operating at the Maturity Level 2 - Defined. Williams Adley identified the following deficiencies within the ISCM IG FISMA metric domain:

i. The CPSC has not implemented an ISCM program in accordance with NIST guidance to support a risk management program based on organizational 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 captured the information necessary to report on the qualitative and quantitative performance measures defined in the ISCM plan.
iii. The CPSC provided the Security Assessment Plans for the five sampled major information systems early enough for an evaluation of those documents. However, the CPSC did not provide the rest of the documentation supporting the CPSC's ATO decisions in a timely enough manner to evaluate. Therefore, Williams Adley was not able to review that documentation or consider those documents in the FISMA evaluation.

Detect Function Recommendations

We recommend that the CPSC:

39. Integrate the established strategy for identifying organizational risk tolerance into the Information Security Continuous Monitoring plan (*Information Security Continuous Monitoring i*).
40. Implement Information Security Continuous Monitoring procedures including those procedures related to the monitoring of performance measures and metrics , that support the Information Security Continuous Monitoring program (*Information Security Continuous Monitoring ii*) (2021 recommendation).
41. Implement Information Security Continuous Monitoring procedures for conducting ongoing authorizations and provide authorizations to operate for all major information systems (*Information Security Continuous Monitoring iii*) (2021 recommendation).

4.4 Respond Function

Progress

In FY 2021, the CPSC made progress in addressing previously identified Incident Response deficiencies. For example, the CPSC has transitioned their SIEM tool for log aggregation and alerting as well as to improve integration with the CPSC's other incident response tools and defined some performance metrics. Overall, the CPSC has made progress on open prior year recommendations, but not enough to close any findings.

Incident Response Conditions

Based on the evaluation procedures performed, Williams Adley determined that the Incident Response IG FISMA metric domain was operating at the Maturity Level 3 - Consistently Implemented. 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. Specifically, the Incident Response Plan does not consistently reflect the United States Computer Emergency Readiness Team (US-CERT) reporting activities (i.e., function impact, information, recoverability) currently in place.
ii. Based on received documentation, the CPSC has some defined metrics (i.e., date and time of incident notification and resolution) but not yet implemented explicit performance measures, outside incident response timing metrics, evaluating the effectiveness of its incident response program and related activities.
iii. The CPSC does report potential incidents, however, the CPSC has not implemented an effective mechanism to evidence timely reporting to US-CERT in accordance with requirements. For example, the one reported incident reported to US-CERT tested was not reported to US-CERT timely.

Respond Function Recommendations

We recommend that the CPSC:

42. Update and implement the CPSC policy and plan with the latest practices, including Incident Response performance measures and implemented profiling techniques (*Incident Response i/ii*).
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*).

4.5 Recover Function

Progress

In FY 2021, the CPSC made some progress in addressing previously identified Contingency Planning deficiencies. For example, the CPSC completed testing the GSS LAN and ITDS/RAM ISCPs in FY 2021. Other ISCP tests were performed but were not available for Williams Adley to review before the end of the fiscal year. The CPSC also has begun implementing Cloud solutions as an approach to improve contingency planning. Overall, the CPSC has made progress on open prior year recommendations, but not enough to close any findings.

Contingency Planning Conditions

Based on the evaluation procedures performed, Williams Adley determined that the Contingency Planning IG FISMA metric domain was operating at the Maturity Level 1 - Ad-hoc. 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. Prior to FY 2021, the CPSC surveyed some of the CPSC program offices to aid them in identifying critical systems while completing the GSS Business Impact Assessment (BIA). However, the BIA does not define the CPSC's mission - essential functions. Further, the BIA states that recovery timing requirements may not be enough 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.
iii. The CPSC has not developed an approach to integrate contingency planning with the other information security domains and requirements, especially risk management. For example, as reported in FY 2020, the CPSC has not developed a Disaster Recovery Plan, and instead has accepted the risk for not doing so. However, it is not clear that this risk acceptance is in line with the CPSC's risk tolerance because the risk tolerance to guide the information security decisions

is not formally defined. Further, although the CPSC has established an alternate storage site, the CPSC has not established an alternate processing site in accordance with the policy requirements. Instead, the CPSC is waiting to utilize Cloud solutions for this purpose once they are fully implemented and authorized to operate.

iv. The CPSC has made updates to two (2) out of five (5) sampled major system's ISCPs and completed tabletop exercises of those ISCPs. However, the CPSC has not clearly defined the required testing procedures and did not integrate testing with other contingency plans. Additionally, the CPSC was not able to produce the ISCP testing results for the Consumer Products Safety Risk Management System.

Recover Function 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 (e.g., National Institute of Standards and Technology (NIST) Special Publications 800-34 and 800-53, Federal Continuity Directive 1, NIST Cybersecurity Framework, and National Archive and Records Administration guidance) (*Contingency Planning i*).
45. Develop, document, and distribute all required contingency planning documents (e.g.. 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/iv*).
46. Integrate documented contingency plans with the other relevant agency planning areas (*Contingency Planning iii*).
47. Test the set of documented contingency plans (*Contingency Planning iv*).

5. CONSOLIDATED LIST OF RECOMMENDATIONS

Table 5-1: Index of Recommendations

Finding	Recommendation
Identify(Risk Management)	1. Develop and implement a process to maintain an up-to-date and complete information system inventory (*Risk Management i*). 2. Develop, document, and implement a process for determining and defining system boundaries in accordance with the National Institute of Standards and Technology guidance (*Risk Management ii/iii*). 3. Establish and implement policies and procedures to manage software licenses using automated monitoring and expiration notifications (*Risk Management ii/iii*). 4. Establish and implement a policy and procedure to ensure that only authorized hardware and software execute on the agency's network (*Risk Management ii/iii*). 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: 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 the CPSC's operational mission, facility, or social media) (*Risk Management ii/iii*). 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 ii/iii*). 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*). 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*). 9. Develop and implement an Enterprise Risk Management (ERM) program based on the National Institute of Standards and Technology and ERM Playbook (Office of Management and Budget 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 iv/v/vi*). 10. Develop and implement a supply chain risk management plan (*Supply Chain Risk Management i*). 11. Develop and implement an information security architecture that supports the Enterprise Architecture. (*Risk Management vii*). 12. Develop an Enterprise Architecture to be integrated into the risk management process (*Risk Management vii*).
Identify(Supply Chain Risk Management)	13. Develop supply chain risk management policies and 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 ii/iii/iv*) (2021 recommendation).
Protect(Configuration Management)	14. Further define the resource designations for a Change Control Board (*Configuration Management i*). 15. Develop and implement a Configuration Management plan to ensure it includes all requisite information (*Configuration Management ii/iii).* 16. Develop, implement, and disseminate a set of Configuration Management procedures in accordance with the inherited Configuration Management Policy which includes the process management follows to develop and tailor common secure configurations (hardening guides) and to approve deviations from those standard configurations (*Configuration Management iv/v*). 17. Integrate the management of secure configurations into the organizational Configuration Management process (*Configuration Management v*). 18. Consistently implement flaw remediation processes, including the remediation of critical vulnerabilities (*Configuration Management vi*). 19. Identify and document the characteristics of items that are to be placed under Configuration Management control (*Configuration Management vii*). 20. Establish measures to evaluate the implementation of changes in accordance with documented information system baselines and integrated secure configurations (*Configuration Management vii*).
Protect(Identity and Access Management)	21. Define and document a strategy (including specific milestones) to implement the Federal Identity, Credential, and Access Management architecture (*Identity and Access Management i/ii/iii*). 22. Integrate Identity, Credential, and Access Management strategy and activities into the Enterprise Architecture and Information Security Continuous Monitoring (*Identity and Access Management i/ii/iii*). 23. 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, and • Description of how cybersecurity is integrated into human resources practices (*Identity and Access Management iv*). 24. Define and implement a process to ensure the completion of access agreements for all CPSC users. (*Identity and Access Management v*). 25. Enforce Personnel Identity Verification card usage for authenticating to all CPSC systems (*Identity and Access Management vi*). 26. Identify and document potentially incompatible duties permitted by privileged accounts (*Identity and Access Management vii*). 27. Document and implement a process to restrict the use of privileged accounts and services when performing non-privileged activities (*Identity and Access Management vii*). 28. Fully deploy the CPSC's privileged access management solution (*Identity and Access Management vii*). 29. Log and actively monitor activities performed while using privileged access that permit potentially incompatible duties (*Identity and Access Management vii*). 30. Define and implement the identification and authentication policies and procedures (*Identity and Access Management ii*). 31. Define and implement processes for provisioning, managing, and reviewing privileged accounts (Identity and Access Management vii) (2021 recommendation).
Protect(Data Protection and Privacy)	32. 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*). 33. Document and implement a process for periodically reviewing for and removing unnecessary Personally Identifiable Information from agency systems (*Data Protection and Privacy i*). 34. Develop and implement data encryption policies and procedures (*Data Protection and Privacy ii*). 35. 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 (*Data Protection and Privacy iii*).
Protect(Security Training)	36. Perform an assessment of the knowledge, skills, and abilities of CPSC personnel with significant security responsibilities (*Security Training i*). 37. Document and implement a process for ensuring that all personnel with significant security roles and responsibilities

	are provided specialized security training to perform assigned duties (*Security Training ii/iii*) (2021 recommendation). 38. 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/v*).
Detect(Information Security Continuous Monitoring)	39. Integrate the established strategy for identifying organizational risk tolerance into the Information Security Continuous Monitoring plan (*Information Security Continuous Monitoring i*). 40. Implement Information Security Continuous Monitoring procedures, including those procedures related to the monitoring of performance measures and metrics , that support the Information Security Continuous Monitoring program (*Information Security Continuous Monitoring ii*) (2021 recommendation). 41. Implement Information Security Continuous Monitoring procedures for conducting ongoing authorizations and provide authorizations to operate to all major information systems (*Information Security Continuous Monitoring iii*) (2021 recommendation).
Respond(Incident Response)	42. Update and implement the CPSC policy and plan with the latest practices, including Incident Response performance measures and implemented profiling techniques (*Incident Response i/ii*). 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*).
Recover(Contingency Planning)	44. Develop and document a robust and formal approach to contingency planning for agency systems and processes using the appropriate guidance (e.g., National Institute of Standards and Technology (NIST) Special Publications 800-34/53, Federal Continuity Directive 1, NIST Cybersecurity Framework, and National Archive and Records Administration guidance) (*Contingency Planning i*). 45. Develop, document, and distribute all required Contingency Planning documents (e.g.. 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/iv*). 46. Integrate documented contingency plans with the other relevant agency planning areas (*Contingency Planning iii*). 47. Test the set of documented contingency plans (*Contingency Planning iv*).

Appendix A. Objective, Scope, and Methodology

A.1 Objective

The objective was to perform an independent evaluation of the CPSC's implementation of FISMA[5] for FY 2021. In support of this objective, Williams Adley conducted the evaluation in accordance with OMB Memorandum 21-02, *Fiscal Year 2020-2021 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 2021. 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
- CPSC Public Website (CPSC.gov)
- International Trade Data System/Risk Automation 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 2021 IG FISMA Reporting 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)

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

FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or source. To ensure the adequacy and effectiveness of these controls, FISMA requires an independent external inspector to perform annual reviews of the information security program. The FY 2021 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 April through October 2021 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 Williams Adley's 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 the 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 following Notice of Findings and Recommendations (NFRs) for each IG FISMA function to CPSC management:

- Identify NFR delivered on July 29, 2021
- Protect NFR delivered on September 22, 2021
- Detect NFR delivered on October 6, 2021
- Respond NFR delivered on October 7, 2021
- Recover NFR delivered on October 4, 2021.

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 2021 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 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

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. 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*.[6] 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:

- 5 Code of Federal Regulations 930.301
- Center for Internet Security Top 20 Critical Security Controls
- Chief Information Officer Council/Chief Acquisition Officer Council, *Cloud Computing Contract Best Practices*
- Department of Homeland Security - *Cybersecurity and Infrastructure Security Agency Trusted Internet Connection 3.0 Core Guidance*
- Department of Homeland Security Binding Operational Directive 18-01
- 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 20-01
- Department of Homeland Security Cyber Incident Reporting Unified Message
- Department of Homeland Security Emergency Directive 19-01
- 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

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

- Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance
- 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 Senior Accountable Officer for Privacy Federal Information Security Modernization Act Metrics
- FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics
- FY 2021 Senior Accountable Officer for Privacy Federal Information Security Modernization Act Metrics
- Homeland Security Presidential Directive 12
- National Cybersecurity Workforce Framework
- National Insider Threat Policy
- 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 8170
- 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 Privacy Framework
- National Institute of Standards and Technology SP 800-30
- National Institute of Standards and Technology SP 800-34
- 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 800-44
- National Institute of Standards and Technology SP 800-50
- National Institute of Standards and Technology SP 800-53, Rev. 4
- National Institute of Standards and Technology SP 800-53, Rev. 5
- National Institute of Standards and Technology SP 800-60
- 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 800-83
- National Institute of Standards and Technology SP 800-84
- National Institute of Standards and Technology SP 800-86
- National Institute of Standards and Technology SP 800-122
- 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 800-163
- National Institute of Standards and Technology SP 800-181
- National Institute of Standards and Technology SP 800-184
- National Institute of Standards and Technology Supplemental Guidance on Ongoing Authorization
- Office of Management and Budget Circular No. A-11
- Office of Management and Budget Circular No. A-123
- Office of Management and Budget Circular No. A-130, Appendix I
- Office of Management and Budget Memorandum 14-03
- Office of Management and Budget Memorandum 15-14
- Office of Management and Budget Memorandum 16-17
- Office of Management and Budget Memorandum 17-12
- 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 19-26
- Office of Management and Budget Memorandum 20-04
- Office of Management and Budget Memorandum 20-32
- Office of Management and Budget Memorandum 21-02
- Presidential Policy Directive – 8
- Presidential Policy Directive – 41
- Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act
- SANS Institute, *Critical Security Controls*
- US-Computer Emergency Readiness Team, *Incident Notification Guidelines*

Appendix B. Management Responses

In response to the Fiscal Year 2021 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. At the same time, staff states that there are existing program functions that are substantially effective. CPSC takes information security and privacy seriously and continues to invest in ongoing program improvements, system modernization, data management, and cloud migration activities to improve agency performance and enhance security. Staff points to the following accomplishments in FY21 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 software and network connectivity required to integrate the agency's systems into the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) SSP 2.0 program.
- Addressed initiatives included in the U.S. Cybersecurity & Infrastructure Security Agency (CISA) alert (AA21-131A) on protecting agency information systems from ransomware attacks. Verified the implementation of 7 of the 11 CISA recommendations; two are partially implemented; and two are currently being addressed.
- Developed and implemented an enterprise system logging capability—which significantly expanded the collection of log events from critical infrastructure components into a centralized repository that allows IT security staff to perform real-time capturing, indexing, and correlating of network security data to produce graphs, actionable alerts, dashboards, and visualizations.
- Implemented requirements included in DHS Binding Operational Directive 20-01, which required all federal agencies to develop and publish a Vulnerability Disclosure Policy (VDP). The VDP helped increase awareness of undetected vulnerabilities within agency public-facing web sites. VDP requires agency IT staff to research and respond to publicly reported vulnerabilities
- Proactively implemented processes to utilize the CISA provided Web Application Scanning (WAS) shared service. WAS performs a monthly scan of agency public-facing web sites to help identify system vulnerabilities and configuration weaknesses as well as provide recommendations for remediating identified vulnerabilities.
- Responded to over 80 Critical Security Advisories—which are security alerts from software vendors, hardware manufacturers, and CISA regarding critical vulnerabilities found in software/hardware systems. These alerts require organizations using affected software/hardware to take immediate action to remediate the vulnerabilities and associated risks.
- Responded to CISA Emergency Directives 21-01, 21-02, and 21-04.
- Responded to requirements included in Presidential Executive Order 14208, Improving the Nation's Cybersecurity.

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 approved 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 two-factor Personal Identity Verification (PIV) card or, as an alternative when PIV cards are lost, damaged, or inactive, an alternative token-based NIST Level of Assurance (LOA) 4 credential.
- The agency's physical access control systems electronically accept and authenticate PIV credentials for physical access to restricted areas in agency offices.
- The agency's systems are scanned regularly for vulnerabilities using Security Content Automation Protocol- (SCAP) validated tools.
- All agency laptops and mobile devices encrypt data at rest.
- Agency users are tested regularly on their understanding and recognition of phishing threats using simulated phishing exercises.
- The agency has fully implemented DHS EINSTEIN tools to detect and block attacks and provide insights to DHS 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.
- The agency provided ransomware training to all agency employees.

In addition, in fiscal year 2021, the agency reported three (3) total incidents to CISA, as required by OMB. One incident involved over 500 DNS alerts sent to the CPSC CSIRT team (which were Page 3 of 3 investigated by CPSC IT security staff and confirmed as false positives); one incident involved the loss of an agency mobile phone; and one incident involved a successful phishing attempt, which resulted in no impact to CPSC information or information systems. The agency had no major incidents in FY2021.

Management believes that the number of deficiencies in the FY 2021 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.

Appendix C. Acronyms

ATO	Authorization to Operate
BIA	Business Impact Assessment
CIGIE	Council of Inspectors General on Integrity and Efficiency
CPSC	U.S. Consumer Product Safety Commission
DHS	Department of Homeland Security
DNS	Domain Name Sever
ERM	Enterprise Risk Management
EXIT	Office of Information and Technology Services
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GSS LAN	General Support System Local Area Network
ICAM	Identity, Credential, and Access Management
IG	Inspector General
ISCM	Information Security Continuous Monitoring
ITDS/RAM	International Trade Data System/Risk Assessment Methodology
ISCP	Information System Contingency Plans
IT	Information Technology
NIST	National Institute of Standards and Technology
NFR	Notice of Findings and Recommendations
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identity Verification
Rev.	Revision
SCRM	Supply Chain Risk Management
SIEM	Security Information and Event Management
SP	Special Publication
US-CERT	United States Computer Emergency Readiness Team
Williams Adley	Williams, Adley, & Co.-DC LLP

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