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

Semiannual Report to Congress

April 1, 2022 to September 30, 2022

October 30, 2022

23-O-02

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.

Top 10 Most Significant Open Recommendations from the Office of Inspector General to the Consumer Product Safety Commission

1. Develop and implement an internal control system covering the operations of its programs. (FMFIA)
2. Develop effective written policies and procedures to govern agency operations. (DIRECTIVES)
3. Develop and implement an Enterprise Risk Management (ERM) program to allow agency officials to utilize risk management principles in the operations of the agency. (FISMA)
4. Ensure that management officials are aware of OIG recommendations that impact their areas of responsibility and actively work toward implementing said recommendations. (BREACH)
5. Improve data management by developing a data governance framework. (NEISS)
6. Improve the effectiveness of agency communication and other outreach efforts by implementing a risk assessment process. (OCM)
7. Develop and implement an effective cost accounting system. (NEISS)
8. Develop and implement written guidance governing the CPSC's use of statements of assurance to meet its requirements under the FMFIA. (BREACH)
9. Develop and implement supply chain risk management policies and procedures. (FISMA)
10. Assess the IT security risks previously identified and develop a corrective action plan that prioritizes addressing the most critical risks and establishes a timeline for taking corrective action. (FISMA)

The Office of Inspector General classifies certain recommendations for corrective action to the agency as significant. The definition used for significant includes those recommendations that have wide programmatic impact or where the implementation would result in a significant financial impact.

MESSAGE FROM THE INSPECTOR GENERAL

I am pleased to submit the Semiannual Report to Congress for the U.S. Consumer Product Safety Commission (CPSC) Office of Inspector General (OIG). This report details the work of the OIG in the oversight of the CPSC for the second half of Fiscal Year (FY) 2022.

My professional and dedicated staff continue to do the work necessary to fight fraud, waste, and abuse at the CPSC while continuing to make findings and recommendations to aid the agency in achieving its mission. We have permanently returned to the office, in a hybrid environment, and completed our work with OPM to design the most efficient organization to provide oversight of the CPSC as it grows and evolves. Unfortunately, agency funding issues have prevented us from hiring the two additional full time positions required to implement our reorganization.

The CPSC continues to operate under a pilot telework program allowing up to four days per week of telework and requiring that employees who telework more than half-time forfeit the right to exclusive use of an office. This pilot program was originally scheduled to end in September; however, it was extended in August to January 31, 2023.

As detailed in both our previous semiannual report and our Audits of the CPSC's Implementation of the Federal Managers' Financial Integrity Act and Grants Program, the CPSC has still not established and implemented a formal internal control program over its operations, nor a more effective cost accounting system.

Additionally, there remains a misalignment between how the CPSC identifies programmatic or operational activities, how it measures the performance of these activities, and how it reports these activities. Without an effective internal control program, the CPSC may not be able to identify and address appropriate risks or measure whether programs are operating as intended. The agency's decision not to provide our office the previously agreed-to full time positions aggravates this risk and hinders our oversight of the agency.

As reported in the prior Semiannual Report, we are concerned that the internal control challenges currently facing the agency may adversely impact the CPSC's utilization of the pandemic related funding Congress has appropriated the CPSC. To date, the CPSC has spent 19.4% of the $50 million appropriated to hire staff and begin the process to enhance targeting, surveillance and screening systems; data collection; and communications.

However, although funding constraints have prevented the agency from adequately resourcing efforts to improve the internal control program in FY 2022, the new Chair has championed an effort to review and revise the agency's directives system. If successfully implemented, this would be a key step in improving internal control across the agency.

Finally, although not implemented as of the end of the reporting period, agency management has taken substantive steps to address the previously reported issue regarding OIG access to agency emails. There is every reason to believe that by the next semiannual report this issue will have been resolved and we will again have the degree of access to agency email that we require to perform our oversight responsibilities.

We look forward to continuing to work with Congress and agency management in order to promote the efficiency and effectiveness of agency programs.

Christopher W. Dentel, Inspector General

Table of Contents

Background

U.S. Consumer Product Safety Commission

The U.S. Consumer Product Safety Commission (CPSC) is an independent federal regulatory agency, created in 1972, by the Consumer Product Safety Act (CPSA). In addition to the CPSA, as amended by the Consumer Product Safety Improvement Act of 2008 (CPSIA), and Public Law No. 112-28, the CPSC administers other laws, such as the Federal Hazardous Substances Act, the Flammable Fabrics Act, the Poison Prevention Packaging Act, the Refrigerator Safety Act, the Virginia Graeme Baker Pool and Spa Safety Act, the Child Safety Protection Act, the Labeling of Hazardous Art Materials Act, the Children's Gasoline Burn Prevention Act, the Drywall Safety Act of 2012, the Child Nicotine Poisoning Prevention Act, and the Nicholas and Zachary Burt Memorial Carbon Monoxide Poisoning Prevention Act of 2022.

The CPSC's mission is "Keeping Consumers Safe." Congress granted the CPSC broad authority to issue and enforce standards prescribing performance requirements, warnings, or instructions regarding the use of consumer products under the CPSA and the CPSIA, as well as numerous other laws.

By statute, the CPSC is headed by five commissioners who are nominated by the president and appointed by and with the advice and consent of the Senate. One of the commissioners is designated by the president and confirmed by the Senate to serve as the Chairman of the CPSC. The chairman is the principal executive officer of the Commission.

This October the CPSC is celebrating 50 years of keeping consumers safe. Since 1972, the CPSC has protected the public from unreasonable risks of injury or death associated with the use of thousands of types of consumer products.

Office of Inspector General

The Office of Inspector General (OIG) is an independent office established under the provisions of the Inspector General Act of 1978 (IG Act), as amended. The CPSC OIG was established on April 9, 1989. Mr. Christopher W. Dentel was named Inspector General in 2004.

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.

We are committed to:

- Working with the Commission and the Congress to improve program management.
- Maximizing the positive impact and ensuring the independence and objectivity of our audits, investigations, and other reviews.

- Using our investigations and other reviews to increase government integrity and recommend improved systems to prevent fraud, waste, and abuse.
- Being innovative, questioning existing procedures, and suggesting improvements.
- Building relationships with program managers based on a shared commitment to improving program operations and effectiveness.
- Striving to continually improve the quality and usefulness of our products.
- Working together to address government-wide issues.

We offer actionable recommendations to increase the efficiency and effectiveness of the CPSC in its mission to protect the public against unreasonable risks of injuries associated with consumer products. We focus our available resources on high-risk areas and continuously seek ways to provide value to our stakeholders.

The OIG continues its commitment to building an integrated planning framework with its risk assessment process. The office conducts annual risk assessments, generally in the first quarter of the fiscal year, of both its own operations as well as the agency as a whole. The OIG uses the results of these assessments to identify the Top Management and Performance Challenges facing the CPSC, as well as to develop its annual audit plan.

Top Management and Performance Challenges Facing the CPSC for FY 2023

1. Internal Control System
2. Enterprise Risk Management
3. Resource Management
4. Information Technology Security

The OIG has recently updated its management challenges to reflect ongoing progress at the CPSC. While the four topics remain the same and the agency has made progress addressing some elements of a topic, new audits and research have brought to light further opportunities for change and progress at the agency. Please see our website for more detail on these challenges to the CPSC in Fiscal Year (FY) 2023.

The OIG remains committed to automating its internal processes to the maximum extent possible. We continue to find/seek new opportunities to integrate administrative functions into our FedRamp compliant cloud-based audit software to free up staff resources to focus on our audit and investigative mission.

Audit Program

During this semiannual period, the OIG completed two audits, reviews, or special projects. At the end of the reporting period, four audits, reviews, or special projects are ongoing.

Reports Completed During this Reporting Period

Review of the CPSC's Compliance with the Payment Integrity Information Act for FY 2021
Transmitted: May 4, 2022
For the full report click here

The OIG contracted with Kearney & Company (Kearney) to perform a review of the CPSC's compliance with the reporting requirements contained in the Payment Integrity Information Act (PIIA), for transactions in FY 2021. The review was performed in accordance with Council of Inspectors General for Integrity and Efficiency (CIGIE) Quality Standards for Inspection and Evaluation (QSIE). The review focused on the CPSC's compliance with the elements identified as criteria in the relevant Office of Management and Budget (OMB) guidance, as well as program internal controls.

Overall, Kearney found that for FY 2021, the CPSC complied with PIIA. In accordance with OMB, all elements must be complied with in order to result in overall compliance.

Evaluation of the CPSC's FISMA Implementation for FY 2022
Transmitted: July 22, 2022
For the full report click here

The OIG contracted with Williams, Adley & Company-DC, LLP (Williams Adley) to review the CPSC's compliance with the reporting requirements of the Federal Information Security Modernization Act (FISMA) for FY 2022. The objective of this review was to determine the effectiveness of the CPSC's information security program in accordance with the FY 2022 FISMA reporting requirements, issued by the Department of Homeland Security and OMB Memorandum (M)-22-05, *Fiscal Year 2021-2022 Guidance of Federal Information Security and Privacy Management Requirements*. As a result of changes in OMB requirements, this year is the first under the new continuous monitoring model. Williams Adley reviewed a subset of 20 "core" metrics that were in scope for FY 2022. The review was performed in accordance with CIGIE QSIE.

Williams Adley found that the CPSC was not compliant with all of FISMA's requirements. However, the CPSC was making progress in implementing many FISMA requirements. Williams Adley made 24 recommendations, 3 of which were new, to improve the CPSC's information security posture.

Ongoing Projects

Human Resources Assessment
The OIG contracted with AE Strategies to evaluate the CPSC's human resources program's ability to provide adequate support to the CPSC as the agency experiences a period of rapid growth. AE Strategies will evaluate the human resources program using the Human Capital Framework evaluation model. This review will be performed using Office of Personnel Management assessment tools designed to measure the effectiveness of the CPSC's human capital program in meeting present and future agency needs.

Audit of the Consumer Product Safety Commission's Fiscal Year 2022 Financial Statements
The OIG contracted with CliftonLarsonAllen, LLP, an independent public accounting firm, to perform an independent audit of the CPSC's financial statements according to all current standards for the period ended September 30, 2022. The objective of this audit is to determine whether the CPSC's financial statements present fairly the financial position of the agency and are compliant with relevant laws and regulations. The CPSC is required to submit audited financial statements in accordance with the Accountability of Tax Dollars Act of 2002, which retroactively implements the Chief Financial Officers Act of 1990 for smaller agencies, including the CPSC. This audit is being performed in accordance with Generally Accepted Government Auditing Standards (GAGAS).

Import Surveillance
The OIG is performing an audit of the internal controls over the CPSC's Import Surveillance program in accordance with GAGAS for the period ended September 30, 2021. The objective of this audit is to assess the design, implementation, and effectiveness of the internal controls over the CPSC's Import Surveillance program and to determine whether the CPSC's import surveillance performance metrics are appropriate and effectively measure CPSC activity to target and assess the safety of imported goods.

Penetration Test
The OIG contracted with Williams Adley, to perform a penetration and vulnerability assessment of the CPSC network. The objective of this penetration test is to assess the security of the CPSC's information technology infrastructure by safely attempting to exploit security vulnerabilities. The review is being performed in accordance with CIGIE QSIE.

Previously Issued Reports with Open Recommendations

Please see Appendix D for a consolidated list of open recommendations.

Consumer Product Safety Risk Management System Information Security Review Report
Transmitted: June 5, 2012
For the full report click here

The objective of this review was to evaluate the application of the Risk Management Framework to the Consumer Product Safety Risk Management System. CPSIA requires the CPSC to implement a publicly accessible and searchable database of consumer product incident reports. The period of the review was December 2010 through February 2011. The work was performed in accordance with CIGIE QSIE. Overall, we found there were several inconsistencies and weaknesses in the security certification and assessment of this database. There were eight consolidated recommendations made with this report and five remain open.

Cybersecurity Information Sharing Act of 2015 Review Report
Transmitted: August 4, 2016
For the full report click here

The objective of this review was to determine whether the CPSC had established the policies, procedures, and practices required by the Cybersecurity Act of 2015 for agency systems that contain Personally Identifiable Information. During this review, we also considered whether standards for logical access were appropriate. The OIG completed this work in accordance with CIGIE QSIE. We found the CPSC had not achieved a number of the requirements set forth in the Cybersecurity Act of 2015 or developed appropriate logical access policies and procedures. There were five consolidated recommendations associated with this report and all five remain open.

Audit of the Telework Program for Fiscal Year 2016
Transmitted: September 29, 2017
For the full report click here

The objectives of this audit were to determine if the CPSC had an effective program in place to capitalize on the benefits of telework, established adequate internal controls over telework, and administered the telework program in accordance with federal laws, regulations, guidance, and agency policy. The audit was performed in accordance with GAGAS. Overall, we found that the agency had a policy; however, it was not entirely effective and did not fully comply with federal laws, regulations, and agency policy. We made nine recommendations to improve the program and five remain open.

Audit of the Occupant Emergency Program for Fiscal Year 2017
Transmitted: June 7, 2018
For the full report click here

The OIG audited the CPSC's Occupant Emergency Program in place for FY 2017. The purpose of an Occupant Emergency Program is to reduce the threat of harm to personnel, property, and other assets within a federal facility in the event of an emergency. The objectives of this audit were to determine program effectiveness and compliance with the *Occupant Emergency Program: An Interagency Security Committee Guide* and other criteria. The audit was performed in accordance with GAGAS. Overall, we found that the CPSC's Occupant Emergency Program was not compliant with government-wide guidance and was not operating effectively. To improve the safety of CPSC employees and other assets we made 12 recommendations and 6 remain open.

Audit of the CPSC'S Directives System
Transmitted: March 21, 2019
For the full report click here

The OIG conducted an audit of the CPSC's Directives System as of March 31, 2018. The objectives of this audit were to determine whether the CPSC's policies and procedures for the Directives System complied with federal regulations and procedures and were effective in helping agency staff meet the CPSC's mission. This audit was performed in accordance with GAGAS. Overall, we found that the CPSC's Directives System was not fully compliant with government-wide requirements, its own policies, or fully effective in helping staff to meet the CPSC's mission. We made two recommendations to improve the Directives System and one remains open.

Review of Personal Property Management System and Practices for the Calendar Year 2017
Transmitted: May 31, 2019
For the full report click here

The OIG contracted with Kearney to perform an assessment of the CPSC's control over personal property. The objective was to obtain an independent review of the controls over personal property items, from initial data entry through routine accounting control to disposal. The review was performed in accordance with CIGIE QSIE. Overall, Kearney found that the CPSC's Personal Property Management System and practices were neither compliant with government-wide guidance nor operating effectively. To improve the CPSC's Property Management System Kearney made 25 recommendations and 15 remain open.

Report on the Penetration and Vulnerability Assessment of CPSC's Information Technology Systems
Transmitted: June 11, 2019
For the full report click here

The OIG contracted with Defense Point Security to perform a penetration and vulnerability assessment of the CPSC network. The objective of this penetration test was to assess the security of the CPSC's information technology infrastructure by safely attempting to exploit security vulnerabilities. The review was performed in accordance with CIGIE QSIE. Overall, Defense Point Security found that the CPSC had not designed its information technology infrastructure to be compliant with government-wide guidance and that its information technology infrastructure was not adequately secure. To improve the CPSC's information technology infrastructure DPS made 40 recommendations and 11 remain open.

Report of Investigation Regarding the 2019 Clearinghouse Data Breach
Transmitted: September 25, 2020
For the full report click here

The OIG was asked to investigate a data breach involving the CPSC's Clearinghouse. We determined that the scope of the data breach exceeded the CPSC's estimate in terms of both duration and quantity. The data breach was caused by a combination of mismanagement and incompetence. CPSC employees caused the data breach by inappropriately releasing confidential information. The CPSC's reliance on Clearinghouse management to assess the scope of the breach led to a minimization of the scope of the data breach and adversely affected the CPSC's efforts to respond to the data breach. We found a near total lack of: supervisory review, documented policies and procedures, and training for non-supervisory and first level supervisory employees carrying out Clearinghouse duties. These problems were compounded by management's lack of integrity regarding the dearth of properly designed and implemented internal controls. For years, agency management signed statements of assurance affirming that there were effective internal controls in place over the Clearinghouse, despite knowing this was not true. We made 40 recommendations and 27 remain open.

Review of NEISS Data Quality and Oversight
Transmitted: November 9, 2020
For the full report click here

The OIG contracted with Kearney to review the CPSC's National Electronic Injury Surveillance System (NEISS) program. The NEISS program creates an average of 350,000 records per year. The data contained in these records can be used to raise consumer awareness of emerging product safety hazards, to support detailed studies that provide data on the number and types of injuries associated with specific products, and to inform standards development. The review

was conducted in accordance with CIGIE QSIE. Kearney determined that the NEISS program did not have an adequate data governance program in place to ensure data quality. Additionally, the CPSC could not provide documentation to establish that a legal opinion was obtained before the CPSC expanded the NEISS program to include data on injuries outside of the CPSC's jurisdiction. Finally, the CPSC could not provide sufficient documentation to support estimated costs charged to other federal agencies as required by the Economy Act when using Interagency Agreements. This review made 12 recommendations to improve NEISS data governance and support the methodology to determine costs charged to other agencies and 4 remain open.

Audit of the CPSC's Office of Communications Management's Strategic Goals
Transmitted: February 19, 2021
For the full report click here

The OIG audited the CPSC's Office of Communications Management's (OCM) strategic goals for FYs 2018 and 2019. The objectives of the audit were to assess OCM's methodology for developing key performance measures, implementing their strategic initiatives, and reporting on the results of the effectiveness of those strategic initiatives. Additionally, we assessed OCM's internal controls over the dissemination of consumer product safety information and collaboration with stakeholders. The audit was conducted in accordance with GAGAS. The OIG determined that OCM met or exceeded their targeted number of communications to the public. However, we identified several areas where OCM's internal controls over its performance reporting could be improved, particularly in the area of tracking communication quality and effectiveness. The OIG made 11 recommendations and 1 remains open.

Evaluation of the CPSC's Implementation of the Federal Data Strategy
Transmitted: April 16, 2021
For the full report click here

The OIG contracted with Williams Adley to perform a review of the CPSC's implementation of the Federal Data Strategy. The objective of this review was to obtain an independent evaluation of the CPSC's implementation of the OMB M-19-18, *Federal Data Strategy - A Framework for Consistency*, and associated OMB-issued action plans. The review was performed in accordance with CIGIE QSIE. Williams Adley found that the CPSC completed the required agency actions described in the most recent action plan published by OMB. The report contained four recommendations and all four remain open.

Review of the CPSC's Equal Employment Opportunity Program
Transmitted: April 27, 2021
For the full report click here

The OIG contracted with GKA, P.C., to perform an independent review of the CPSC's Equal Employment Opportunity (EEO) program. The objectives of this review were to determine whether the EEO program complied with all statutory requirements and to assess the accuracy,

completeness, and reliability of the information EEO reported to the U.S. Equal Employment Opportunity Commission. This review was performed in accordance with CIGIE QSIE. The report contained four recommendations to strengthen the program and all four remain open.

Audit of the CPSC's Position Designation and Suitability Program
Transmitted: April 29, 2021
For the full report click here

The OIG audited the CPSC position designation process. Each covered federal position is required to have a designation level (Tier 1 through Tier 5), depending on the sensitivity and risk level of the position. The objectives of this audit were to determine whether all positions in the CPSC were appropriately designated and whether all CPSC employees and contractors have the appropriate background investigation completed. The audit was performed in accordance with GAGAS. The audit identified $49,631 in questioned costs.[1] The OIG made 13 recommendations and 11[2] remain open. The agency did not concur with one recommendation.

Audit of the CPSC's Implementation of FMFIA for FYs 2018 and 2019
Transmitted: May 12, 2021
For the full report click here

The OIG contracted with Kearney to perform an audit of the CPSC's compliance in FYs 2018 and 2019 with the Federal Managers' Financial Integrity Act (FMFIA). Kearney was also charged with evaluating the effectiveness of the CPSC's processes to assess internal control over program operations, as reported in the Chairman's Management Assurance Statement in the Agency Financial Report. The review was performed in accordance with GAGAS. Kearney determined that the CPSC did not comply with the FMFIA in FYs 2018 and 2019. Specifically, a misalignment existed between how the CPSC identified programmatic or operational activities, how it measured the performance of these activities, and how it reported these activities. Additionally, although the CPSC implemented metrics to monitor the performance of its strategic goals and objectives, it did not establish and implement a formal internal controls program over its operations as required by the Government Accountability Office's, *Standards for Internal Control in the Federal Government*, and OMB Circular A-123, *Management's Responsibility for Internal Control*. The report made seven recommendations and seven remain open.

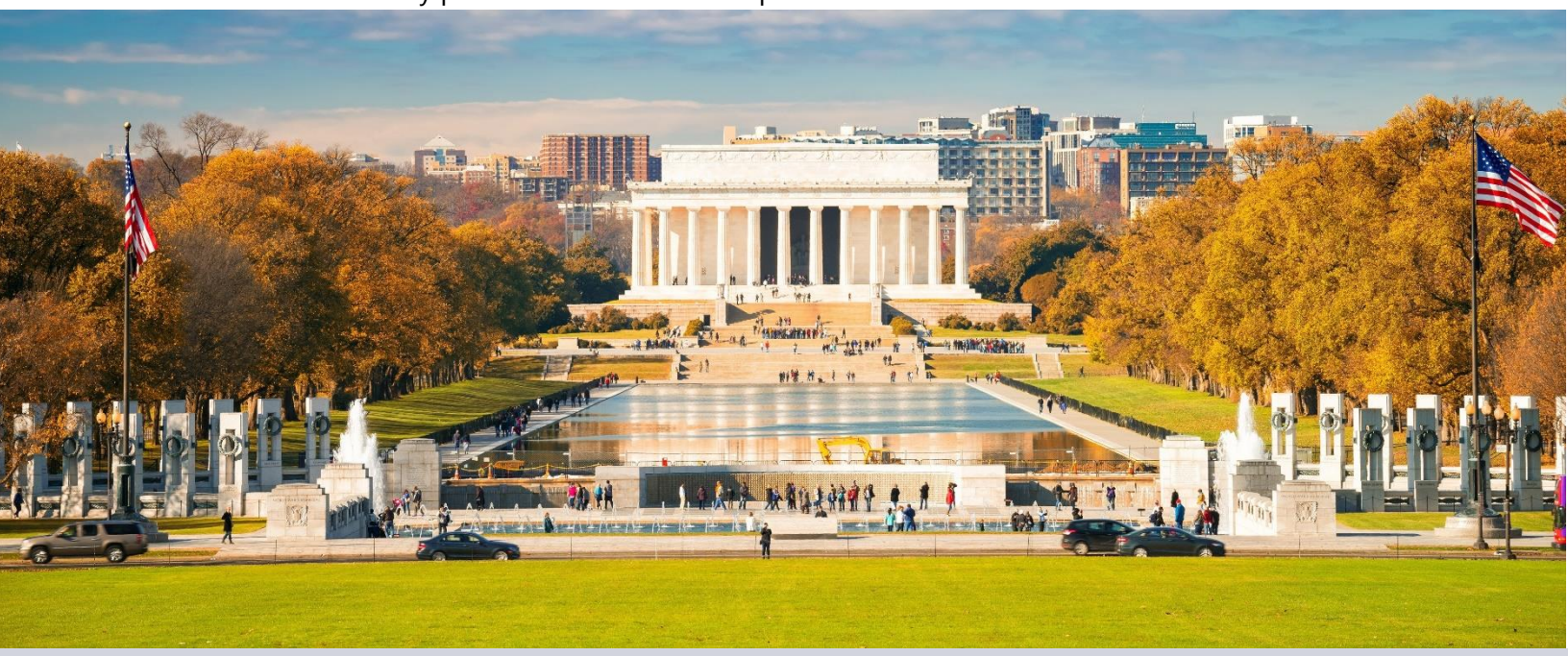
[1] Questioned costs are those costs that are questioned by the CPSC OIG because of an alleged violation of a provision of a law, regulation, contract, grant, cooperative agreement, or other agreement or document governing the expenditure of funds; costs not supported by adequate documentation; or a finding that the expenditure of funds for the intended purpose is unnecessary or unreasonable.
[2] One recommendation from this audit is no longer monitored due to agency disagreement with the recommendation.

Evaluation of the CPSC's FISMA Implementation for FY 2021
Transmitted: October 29, 2021
For the full report click here

The OIG contracted with Williams Adley to review the CPSC's compliance with the reporting requirements of FISMA in FY 2021. The objective of this review was to determine the effectiveness of the CPSC's information security program in accordance with the FY 2021 FISMA reporting requirements issued by the Department of Homeland Security and OMB M-21-02, *FY 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*. The review was performed in accordance with CIGIE QSIE. Williams Adley found that the CPSC was not compliant with all of FISMA's requirements. However, the CPSC was making progress in implementing many FISMA requirements. There were 47 recommendations associated with this report and 40 remain open.

NIST Cybersecurity Framework
Transmitted: January 18, 2022
For the full report click here

The OIG contracted with Williams Adley to perform a review of the CPSC's implementation of the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). The objective of this requirement was to obtain an independent evaluation of the CPSC's implementation of the NIST CSF. The review was performed in accordance with CIGIE QSIE. Williams Adley found that the CPSC had developed a high-level action plan for the NIST CSF in 2017, however, the CPSC had not implemented that plan. Williams Adley made five recommendations to meet the requirements set forth by the NIST CSF and improve the CPSC's information security posture and five remain open.



Investigative Program

The OIG investigates complaints and information received from the CPSC's employees, other government agencies, and members of the public concerning possible violations of laws, rules, and regulations, as well as claims of mismanagement, abuse of authority, waste, and fraud. The objectives of this program are to maintain the integrity of the CPSC and ensure individuals of a fair, impartial, and independent investigation.

Several individuals contacted the OIG directly during the reporting period to discuss their concerns about matters involving CPSC programs and activities. During the reporting period the OIG did not complete any investigations involving a senior government employee where allegations of misconduct were substantiated nor did the OIG receive any actionable allegations of whistleblower retaliation. The table below summarizes the disposition of complaints and investigative work performed from April 1, 2022, through September 30, 2022.

Investigation Status	Count
Open as of April 1, 2022	**6**
Opened during reporting period	33
Closed during reporting period	3
Transferred to other Departments/Agencies	33
Referred to Department of Justice for criminal prosecution	0
Referred for State/Local criminal prosecution	0
Total Indictments/Information from prior referrals	0
Open as of September 30, 2022	**3**

In developing the above statistical table, each case was entered into the appropriate rows based on its ultimate outcome.

Reportable Investigations

2022-I-003 Complaint alleged it was improper for the Office of General Counsel to nullify the Commissioners' vote over a procedural matter. Based on the available information we decided to investigate the following matters: 1) the authority and propriety of the Office of General Counsel to nullify the FY 2022 Operating Plan vote due to a procedural violation; 2) the origin of the nullification course of action; 3) the propriety of the Commissioners' votes on the FY 2022 Operating Plan; 4) the origin of the unauthorized release of the privileged legal review to the Washington Post. The complaint is currently under investigation.

Other Activities

Legislation and Regulatory Review

The OIG reviews internal and external regulations and legislation that affect the OIG specifically, or the CPSC's programs and activities generally. The following were reviewed and commented upon during the reporting period:

Anti-Deficiency Act
Commission Decision Making Procedures
Consolidated Appropriations Act 2021 and 2022
Consumer Product Safety Act
Consumer Product Safety Commission Regulations
Consumer Product Safety Improvement Act of 2008
Coronavirus Aid, Relief, and Economic Security Act (CARES Act)
Economy Act
Ethics Regulations
Executive Order 13932
Federal Acquisition Regulations
Federal Travel Regulations
Freedom of Information Act
Good Accounting Obligation in Government Act
Inspector General Act of 1978, as amended
Maryland Attorneys' Rules of Professional Conduct
Office of Management and Budget Circulars and Memoranda
Office of Personnel Management Classification Standards
Peer Review Guides
Privacy Program
Prohibited Personnel Practices
Public Disclosure of Information, 15 U.S.C. 2055
Purpose Act
Quality Standards for Inspection and Evaluation
Records Management Policies and Regulations
Standards of Conduct for Government Employees
Whistleblower Protection Enhancement Act

OIG Coordination

COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY

The Inspector General maintains active membership in CIGIE and its associated subcommittees. CIGIE identifies, reviews, and discusses issues that are of interest to the entire OIG community. The Inspector General serves on the Audit, Legislation, and Inspection and Evaluation Committees, the Audit Peer Review Subcommittee, and as an adjunct instructor for the CIGIE Training Institute. The Inspector General regularly attends meetings held by CIGIE and their joint meetings with the Government Accountability Office.

The OIG's staff attended seminars and training sessions sponsored or approved by CIGIE. OIG staff are also active participants in a variety of CIGIE subgroups including but not limited to the Deputy Inspectors General group, the management and planning group, and groups covering topics such as investigations, information technology, FISMA, PIIA, and financial statement audits.

COUNCIL OF COUNSELS TO THE INSPECTORS GENERAL

The Counsel to the Inspector General is a member of the Council of Counsels to the Inspectors General (CCIG). The CCIG considers legal issues of interest to the Offices of Inspectors General. During the review period, the Counsel met with peers to discuss items of mutual interest to all OIGs. The Counsel also participates in the CCIG employment law working group, CCIG Investigative Counsel working group, Freedom of Information Act working group, and Small OIG Counsel group.

Instances of CPSC Interference with OIG Access

Section 5(a)(21) of the Inspector General Act of 1978, as amended, requires a detailed description of any attempt by the establishment (in this instance the CPSC) to interfere with the independence of the agency's OIG. This potential interference includes budget constraints designed to limit the OIG's capabilities and incidents where the agency resisted OIG oversight or delayed OIG access to information. During this reporting period, the OIG continues to experience agency interference with access to information.

On August 12, 2021, the Chief Information Officer (CIO) informed the Inspector General that the Office of Information and Technology Services (EXIT) was adopting a new policy regarding access to email systems and would no longer allow the OIG to directly access and search agency email. The stated reason for this change was the CPSC's desire to prevent individuals other than EXIT staff from having access to the CPSC's email system. However, EXIT continues to allow contractors to maintain the access now being denied the OIG. The CIO's proposal was to have EXIT staff conduct searches relating to OIG investigations and require that we inform the CIO and/or a Deputy Executive Director of the details of our requests for searches. This would impinge on OIG independence and violate both the privacy and due process rights of the subjects and witnesses involved in our investigations.

This issue was raised to then acting Chairman Adler in the summer 2021. He chose to accept the CIO's position and continued to deny the OIG direct access to agency email for use in investigations. To allow our office to resume its work until the matter could be more appropriately resolved, we reluctantly agreed to allow an agency information technology specialist to conduct email searches on our behalf with no coordination or sharing of information regarding same with the CIO or Deputy Executive Director.

This issue was raised with the current Chair. He has proposed a solution whereby the OIG uses a Department of Justice contractor to access agency records and perform a search on behalf of the OIG. Currently, the OIG is working with the Office of the Executive Director to finalize procedures and is looking forward to resolving this issue.

Significant Management Decisions with which the Inspector General Disagrees

Section 5(a)(12) of the Inspector General Act of 1978, as amended, requires reporting of any significant management decision with which the Inspector General disagrees. The CPSC has received $50 million in American Rescue Plan Act of 2021 (ARPA) funding as well as receiving additional funding for its grant program. Further, the CPSC is seeking a substantial increase in funding over the next several years in order to allow it to better deal with evolving issues related to consumer safety. In order to provide adequate oversight for FY 2022 this office sought and received agency approval to receive an additional fulltime equivalent position to provide organic oversight of agency programs including the use of ARPA funds in FY 2022.

The agency received substantially less annual budgetary funding for FY 2022 than had been anticipated. As a result, this office did not receive the requested position but did receive additional contract funding. Although we acknowledge the fiscal challenges facing the agency, we feel it is shortsighted to cut oversight at a time when the agency is facing increased oversight challenges. One of the problems created by our lack of staffing is an inability to properly monitor contract work. This is only exacerbated by increasing the amount of contract work. Examples of the areas that would benefit from additional organic oversight include ensuring that the CPSC's ARPA funding is used effectively and in accordance with the criteria provided by Congress, as well as monitoring the operations of its grant programs. And while we understand the agency's inclination to provide money for contract work, what this offices needs is the expertise and knowledge that is built by hiring an employee and training them in the day to day operations of the CPSC. This office maintains that this can be done by repurposing those contract dollars to support our requested full time position.

The need for additional oversight is heightened due to the fact that both the ARPA funds and grant programs represent high risk areas to the CPSC. The ARPA funding's risk factors include its relative size to the agency's budget as a whole and the specificity of the associated congressional criteria for its use. These risks are aggravated by the CPSC's ongoing challenges involving internal control and cost accounting. The grants process is inherently risky due to the complexity of the grant rules and the possibility of fraud. These risks are compounded by the relative lack of agency experience dealing with grants and the new grant program recently added to their portfolio. We have begun an audit which addresses two of the ARPA target areas. However, we do not have the required staff to address any additional ARPA areas at this time.

Appendix A: Cross-Reference to IG Act Reporting Requirements

Citation	Reporting Requirements	Page(s)
Section 4(a)(2)	Review of legislation and regulations.	13
Section 5(a)(1)	Significant problems, abuses, and deficiencies.	4
Section 5(a)(2)	Recommendations with respect to significant problems, abuses, and deficiencies.	4
Section 5(a)(3)	Prior significant recommendations on which corrective action has not been completed.	6-11, 22-28
Section 5(a)(4)	Summary of matters referred to prosecutorial authorities and results.	NA
Section 5(a)(5)	Summary of each report made to head of agency when information was refused.	NA
Section 5(a)(6)	List of audit, inspection, and evaluation reports by subject matter, showing dollar value of questioned costs and of recommendations that funds be put to better use.	NA
Section 5(a)(7)	Summary of each particularly significant report.	4
Section 5(a)(8)	Table showing the number of audit, inspection, and evaluation reports and dollar value of questioned costs for reports.	NA
Section 5(a)(9)	Table showing the number of audit, inspection, and evaluation reports and dollar value of recommendations that funds be put to better use.	NA
Section 5(a)(10)	Summary of each audit, inspection, and evaluation report issued before this reporting period for which no management decision was made by the end of the reporting period, no establishment comment was returned within 60 days; or for those with any outstanding unimplemented recommendations, including the potential aggregate cost savings.	6-11, 22-28
Section 5(a)(11)	Significant revised management decisions.	NA
Section 5(a)(12)	Significant management decisions with which the Inspector General disagrees.	16
Section 5(a)(13)	Information under section 804(b) of Federal Financial Management Improvement Act of 1996.	NA
Section 5(a)(14)	Results of peer review.	18
Section 5(a)(15)	Outstanding recommendations from any peer review conducted by another OIG.	NA
Section 5(a)(16)	Any peer reviews performed of another OIG.	18
Section 5(a)(17)	Statistical table showing total number of investigative reports, referrals, and results of referrals.	12
Section 5(a)(18)	Metrics used to develop data for table in section 5(a) (17).	12
Section 5(a)(19)	Report on each investigation involving a senior government official where allegations of misconduct are substantiated.	NA
Section 5(a)(20)	Detailed description of whistleblower retaliation.	NA
Section 5(a)(21)	Detailed description of attempt to interfere with OIG independence.	15
Section 5(a)(22)	Detailed description of every inspection, evaluation, and audit closed and not publicly disclosed, and every investigation of senior government employee closed and not publicly disclosed.	NA

Appendix B: Peer Reviews

The OIG has in the past completed work under both GAGAS and CIGIE QSIE. Each standard-setting body requires the organization to obtain an external review of its system of quality control every three years and make the results publicly available. The OIG continues to perform work utilizing GAGAS but now only utilizes CIGIE QSIE for work that is contracted out.

GAGAS Peer Reviews

On February 24, 2020, the Corporation for National and Community Service Office of Inspector General issued a report of its External Peer Review of our audit organization and opined that our system of quality control for the year ending September 30, 2019, had been "suitably designed and complied with to provide the CPSC OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects." Audit organizations can receive a rating of pass, pass with deficiencies, or fail. We received an External Peer Review rating of pass. A copy of this peer review is on our website.

The CPSC OIG last completed a peer review on March 20, 2019, for the United States International Trade Commission OIG. We gave the United States International Trade Commission OIG an External Peer Review rating of pass.

The CPSC is currently performing a peer review of the Library of Congress.

Inspection and Evaluation Peer Reviews

On August 25, 2020, the Pension Benefit Guaranty Corporation Office of Inspector General issued a report of its Modified External Peer Review of our Inspections and Evaluations organization and opined that our internal policies and procedures for the period ending June 30, 2020, were current and consistent with covered CIGIE QSIE standards. The seven required standards are Quality Control, Planning, Data Collection and Analysis, Evidence, Records Maintenance, Reporting, and Follow-up. The External Peer review was changed to a Modified Peer Review due to the impact and logistics of doing field work during a pandemic. For the full report click here.

The CPSC is currently receiving a peer review from the Architect of the Capitol.

Appendix C: Statement Regarding Plain Writing

We strive to follow the Plain Writing Act of 2010. The Act requires that government documents be clear, concise, well-organized, and follow other best practices appropriate to the subject or field and intended audience. The abbreviations we use in this report are listed below.

Table of Abbreviations	
ARPA	American Rescue Plan Act of 2021
CCIG	Council of Counsels to the Inspectors General
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CPSA	Consumer Product Safety Act
CPSC or Commission	U.S. Consumer Product Safety Commission
CPSIA	Consumer Product Safety Improvement Act of 2008
EEO	Office of Equal Employment Opportunity and Minority Enterprise
EXIT	Office of Information and Technology Services
FISMA	Federal Information Security Modernization Act
FMFIA	Federal Managers' Financial Integrity Act
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
IG Act	The Inspector General Act of 1978, as amended
Kearney	Kearney & Company
M	Memorandum
NEISS	National Electronic Injury Surveillance System
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
OCM	Office of Communications Management
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIIA	Payment Integrity Information Act
QSIE	Quality Standards for Inspection and Evaluation
Williams Adley	Williams, Adley & Company-DC, LLP

Appendix D: Status of Recommendations

Only 22 recommendations were closed during the current reporting period, down from 45 in the previous one. There appear to be a number of reasons for this reduction. Funding constraints caused the agency to terminate planned efforts to utilize contractors to aid staff in designing and implementing a more effective agency-wide internal controls program. If implemented, this contract effort offered an opportunity to make systemic improvements across the agency that would have positively affected a number of recommendations. On a positive note, the Chair has championed a new effort to review and revise the agency's directive's system.

Due to the relationship between the directives system and agency internal controls, in the short term, the emphasis placed on revising the directives system may result in a delay in the closing of a number of individual recommendations. This is due to both the amount of effort required to overhaul the current system and the need to incorporate internal control changes of individual programs into the overall revised directives system. If successfully designed and implemented, a revised directives system has the potential to greatly improve agency operations and internal controls as well as serving as a key component in closing multiple recommendations.

The Inspector General also notes that the total number of recommendations in this Appendix has increased substantially due to a change in the FISMA audit reporting process. Previously, the OIG had tracked and closed these recommendations as part of the annual FISMA reporting process. Now, only a revolving subset of recommendations will be addressed as part of the annual FISMA review and the OIG will track all FISMA recommendations through the follow-up process.

This chart provides a summary of reports with open recommendations as of the end of the semiannual period and shows progress made during the last six months.

Summary of Recommendation Implementation Progress							
Report Short Title	**Report Date**	**Total Recommendations**	**Closed Prior to April 1, 2022**	**Open as of April 1, 2022**	**Closed during the period**	**Open as of September 30, 2022**	**Total Days Past Due as of September 30, 2022**
RMS	6/5/2012	8	3	5	0	5	3589
CYBER	8/14/2016	5	0	5	0	5	2058
TELEWORK	9/29/2017	9	4	5	0	5	1647
OEP	6/7/2018	12	6	6	0	6	1396
DIRECTIVES	3/21/2019	2	1	1	0	1	1109
PROPERTY	5/31/2019	25	7	18	3	15	1038
PENTEST	6/11/2019	40	27	13	2	11	1027
GRANTS	9/25/2020	22	21	1	1	0	-
BREACH	9/25/2020	40	6	34	7	27	555
NEISS	11/9/2020	12	6	6	2	4	510
OCM	2/19/2021	11	10	1	0	1	408
FDS	4/16/2021	4	0	4	0	4	352
EEO	4/27/2021	4	0	4	0	4	341
PD*	4/29/2021	13	1	12	0	11	339
FMFIA	5/12/2021	7	0	7	0	7	326
FISMA 21	10/29/2021	47	0	47	7	40	156
NIST CSF	1/18/2022	5	0	5	0	5	74
		266	**92**	**174**	**22**	**151**	

*One recommendation from this audit is no longer monitored due to agency disagreement with the recommendation.

The table on the next page shows all open recommendations as of the end of the current semiannual period.

Reports With Open Recommendations

Consumer Product Safety Risk Management System Information Security Review Report (RMS)

June 5, 2012

RMS-1. Identify the participants of the CPSC Risk Executive Council and define specific tasks/milestones for implementing the proposed Risk Management Framework.
RMS-2. Develop an Enterprise Architecture that includes a comprehensive IT security architecture using the CIO Council's guidance and incorporate this into the Security Control Documents.
RMS-3. Fully document the implementation of the security controls.
RMS-4. Update the CPSRMS SSP to be the single authoritative system security document.
RMS-8. Define the specific Public Access controls in place/planned.

Cybersecurity Information Sharing Act of 2015 Review Report (CYBER)

August 14, 2016

Cyber-1. Management updates, develops, and publishes general access control and logical access control policies and procedures for all systems that permit access to PII.
Cyber-2. Provide training or document training completion by individual system owners on establishing, implementing, and maintaining logical access policies and procedures for systems that contain PII.
Cyber-3. The General Access Control Policy and attendant procedures should be updated to include the elements outlined in the report.
Cyber-4. Develop, document, and maintain a software inventory including license management policies and procedures.
Cyber–5. Comply with and enforce HSPD-12 multifactor authentication supported by the Personal Identity Verification Card.

Audit of the Telework Program for Fiscal Year 2016 (TELEWORK)

September 29, 2017

Telework-1. Develop and implement a telework policy that is compliant with current federal laws, regulations, and OPM best practices where appropriate.
Telework-2. Align agency practice and telework policy regarding employee participation and position eligibility.
Telework-3. Document all decisions made with regard to position eligibility, individual participation including policy exceptions, participation limits, and termination of telework agreements.
Telework-4. Design and implement a process to ensure that telework files are complete and regularly reviewed, at least biennially.
Telework-5. Implement a process to validate telework information reported to outside parties and used for internal decision-making to internal source data on a routine basis.

Audit of the Occupant Emergency Program for Fiscal Year 2017 (OEP)

June 7, 2018

OEP-1. Clearly define all the roles to be used in the agency's OEP.
OEP-6. Develop and implement an effective OEP team training program with drills and exercises to include all team members at least annually.
OEP-8. Develop and implement procedures to address the needs of individuals requiring additional assistance. These procedures should include a process to routinely update the list of persons requiring assistance.
OEP-9. Develop and implement procedures to maintain, retain, and update OEP program documents at least semiannually.
OEP-10. Develop and implement an annual round-table discussion with OEP coordinators and teams.
OEP-11. Develop and implement facility-specific policies and procedures.

Audit of the CPSC'S Directives System (DIRECTIVES)

March 21, 2019

Directives-2. Ensure directives are updated to align with the current directives system policies and procedures as well as reflect the current CPSC organizational structure and operations.

Reports With Open Recommendations

Review of Personal Property Management System and Practices for the Calendar Year 2017 (PROPERTY)

May 31, 2019

PMS-7. Develop and implement controls to ensure that the data entered into PMS and IFS is accurate and consistent with CPSC policies and procedures.
PMS-8. Develop procedures to review applicable regulations and laws on an annual basis in order to ensure the property management policies and procedures remain accurate and complete.
PMS-9. Perform and document a formal analysis on the PMS operating environment and system mission to determine the appropriate system categorization for PMS.
PMS-10. Upon a justifiable determination of the PMS system categorization, design, implement, and assess the PMS security controls and formally authorize PMS to operate in accordance with CPSC organizational security policies and procedures as well as other applicable government standards.
PMS-11. Establish and implement POA&M management procedures to ensure that all identified security weaknesses, including PMS application-specific and inherited control weaknesses, are fully documented and tracked.
PMS-13. Establish and implement POA&M management procedures to ensure that changes to estimated completion dates should be documented and reflected in the POA&M tracker.
PMS-14. Estimated completion dates should be documented and reflected in the POA&M tracker.
PMS-15. Perform and document a formal analysis of PMS's operating environment and system mission to determine the appropriate risk level categorization for PMS.
PMS-16. Upon a justifiable determination of PMS's system categorization, design and implement standard procedures for requesting and approving user access to roles and resources in PMS.
PMS-20. Perform and document a risk analysis to identify SoD conflicts that may exist between PMS and other CPSC systems.
PMS-21. Upon completion of the risk analysis, develop and implement procedures to ensure that CPSC users do not have unmonitored conflicting access across multiple systems.
PMS-22. Perform and document a risk analysis to identify potential SoD conflicts within PMS.
PMS-23. Upon the completion of the risk analysis noted above, management should develop and implement procedures that ensure PMS users do not have sufficient access to allow the unmonitored execution of incompatible transactions.
PMS-24. Update and implement configuration change management procedures which include requirements to perform and document quality control reviews.
PMS-25. Develop and implement procedures to log, track, and maintain a list of changes made to the PMS application.

Penetration and Vulnerability Assessment of CPSC's Information Technology Systems (PENTEST)

June 11, 2019

PT-1. REDACTED
PT-2. REDACTED
PT-7. REDACTED
PT-12. REDACTED
PT-13. REDACTED
PT-17. REDACTED
PT-18. REDACTED
PT-20. REDACTED
PT-29. REDACTED
PT-35. REDACTED
PT-36. REDACTED

REPORT OF INVESTIGATION REGARDING THE 2019 CLEARINGHOUSE DATA BREACH (BREACH)

Transmitted: September 25, 2020

BREACH-1. Reconvene the BRT to assess the full extent of the breach, and base its response on the totality of the breach.
BREACH-2. Establish blanket purchase agreements for identity monitoring, credit monitoring, and other related services for data breach victims.
BREACH-3. Complete and publish a document describing lessons learned after the BRT completes its work related to this breach.
BREACH-4. Complete and document annual tabletop exercises. The tabletop exercises test the breach response plan and help ensure that members of the team are familiar with the plan and understand their specific roles. Tabletop exercises should be used to practice a coordinated response to a breach, to further refine and validate the breach response plan, and to identify potential weaknesses in the agency's response capabilities.
BREACH-5. Conduct an annual Breach Response Policy plan review.
BREACH-6. Establish and complete an annual schedule to review blanket purchase agreements for adequacy, complete and document the tabletop exercise, and publish the updated annual Breach Response Policy plan review.
BREACH-12. Review all available data and establish an accurate identification of all data inadvertently released, internally and externally, from 2010 to 2019.
BREACH-13. Obtain an independent review of a sample of Clearinghouse responses prior to 2010 to determine the need for an expanded scope of the review.
BREACH-14. Establish policies and procedures to ensure that when the agency reports data related to a data breach or other violation of law or regulation, the reported data has been independently verified by a person outside of the responsible organization.
BREACH-15. Establish a process for communicating and enforcing the implementation of recommendations previously agreed to by management, as required by law.
BREACH-17. Implement a single data extraction tool to allow maximum functionality in searching multiple product codes while adequately blocking protected data from release. This tool should default to block ALL fields which may contain 6(b) information and PII data. This data tool must contain a standardized data dictionary to limit placement of restricted information to identified fields.
BREACH-18. Once the new tool in Recommendation 17 is implemented, turn off and remove all other data extraction tools from the CPSC inventory of available IT tools.
BREACH-19. Limit access to the underlying database and the data extraction tool to those with a bona fide need for access.
BREACH-22. Annually update and require refresher training for all Clearinghouse staff on the use of the data extraction tool and policies and procedures for accomplishing Clearinghouse work, up to and including the AED for EPHA.
BREACH-23. Develop, disseminate, provide training, and implement policies and procedures on how to use this new data extraction tool to all Clearinghouse staff, up to and including the AED for EPHA. These policies must include step-by-step instructions and checklists to aid staff in completing routine tasks. These policies must include guides and checklists for supervisory review of Clearinghouse staff work.
BREACH-24. Require additional training for Clearinghouse supervisory staff, up to and including the AED for EPHA, on effective review of Clearinghouse staff output.
BREACH-25. Annually update and require refresher training for Clearinghouse supervisory staff, up to and including the AED for EPHA, on the effective review of Clearinghouse staff output.
BREACH-26. Develop, implement, and require training for all Clearinghouse staff, up to and including the AED for EPHA, on a tracking system to monitor Clearinghouse receipt and fulfillment of all Clearinghouse data requests.
BREACH-27. Require supervisory review of all completed Clearinghouse data requests.
BREACH-29. Require initial and annual refresher training for all staff on the importance of protecting 6(b) information and PII, including the rights of individuals and businesses, and how to recognize 6(b) information and PII in documents and how to securely handle this information.
BREACH-30. Enforce Principle of Least Privilege and limit access to data on the P-drive to individuals with a bona fide "need to know."
BREACH-32. Determine, document, and implement a structure for the Clearinghouse.
BREACH-34. Require the Office of Human Resources Management (Human Resources) to provide consultation to ensure that the organizational structure in EPDSI meets the current operational needs, meets span of control best practices, and perform a skills gap analysis. Human Resources will provide a written report of its findings.
BREACH-35. Implement the recommendations from the Human Resources study.
BREACH-37. Design, document, and implement control activities to respond to the results of the completed risk assessment process.
BREACH-38. Develop and implement written guidance on the importance of the statements of assurance process and the related documentation requirements.
BREACH-40. Consider disciplinary action for the supervisors who did not accurately report the status of internal controls in the statements of assurance they produced. Document the results of the disciplinary review, to include the analysis supporting any decision to not perform disciplinary action.

Reports With Open Recommendations

Review of the National Electronic Injury Surveillance System Data (NEISS)

November 9, 2020

NEISS-4. Report to the OIG as to whether an Anti-Deficiency Act violation occurred.
NEISS-5. Stop incurring costs on behalf of other federal agencies in support of the NEISS program based upon a legal determination as recommended in Finding 1, if applicable.
NEISS-6. Develop and implement an effective process to ensure that estimated costs identified in Interagency Agreements are properly supported and representative of "the actual costs of goods or services provided."
NEISS-11. Update and provide training on a routine basis, preferably annually, to address issues found in data entry since the last training.

Audit of CPSC's Office of Communications Management Strategic Goals (OCM)

February 19, 2021

OCM-10. Implement a risk assessment process to determine where to focus efforts in terms of usefulness and improving message effectiveness.

Evaluation of the CPSC's Implementation of the Federal Data Strategy (FDS)

April 16, 2021

FDS-1. Establish a data strategy implementation project plan with milestones that consider mission priorities and current and expected staffing levels to track the progress of the data management program maturation against the current Data and Analytics Strategy Implementation Plan.
FDS-2. Develop and implement a Data Quality Plan that supports the collection and maintenance of data related to identified key CPSC open data sets.
FDS-3. Identify and assign responsibilities to all of the resources who have data governance roles and responsibilities. These resources should include, at a minimum, data owners and data stewards, and those resources should be trained on their responsibilities.
FDS- 4. Dedicate resources to the data management program based on a needs assessment, which should be revisited as the FDS action plans are published. Supplementary resources to consider adding may include data architects, data scientists, data analysts, and training resources.

Review of the CPSC's Equal Employment Opportunity Program (EEO)

April 27, 2021

EEO- 1. Establish policies and procedures that require and document alternative dispute resolution training for all the agency managers and supervisors.
EEO- 2. Establish a regular interval for alternative dispute resolution training, preferably at least annually.
EEO- 3. Enforce counselor, investigator, and Alternative Dispute Resolution training requirements in accordance with EEOC Management Directive 110.
EEO- 4. Implement written policies and procedures to document and maintain independent contractor training compliance with EEOC Management Directive 110. The documentation should, at a minimum, include the name of the trainee, the nature and type of training, the provider, and the date of training. For neutrals the documentation should include evidence of practical training and references.

Reports With Open Recommendations

Audit of the CPSC's Position Designation and Suitability Program (PD)[3]

April 29, 2021

PD-1. Update and implement EXRM directives, policies, and procedures regarding position designation to reflect current EXRM operations and address current OPM policies and guidelines.
PD-2. Develop and maintain an accessible database with all information required to effectively manage the position designation and suitability program. At a minimum, this system should contain the name of the employee or contractor, position number and title, position designation, tier of background investigation completed, entry-on-duty date, date the background investigation was requested, date the background investigation was completed, whether it was an initial investigation or reinvestigation, whether reciprocity was applied, and reinvestigation due date.
PD-4. Use the information developed in Recommendation Two to track an employee's investigation versus the designation of their position and ensure they are properly aligned.
PD-5. Use an automated tool to track when employee and contractor reinvestigations are due.
PD-6. Update the investigations of employees whose completed investigation has exceeded the five-year reinvestigation requirement.
PD-7. Allocate the appropriate resources going forward to ensure that all reinvestigations are initiated on or before the due date.
PD-9. Develop a formal documented process (directive or standard operating procedure) for onboarding contractors.
PD-10. Develop a system to communicate any changes in the onboarding process to contracting officer's representatives and other personnel involved in the onboarding of employees and contractors.
PD-11. Develop and document a systematic and repeatable risk assessment process to evaluate the risk of applying reciprocity for incoming contractors.
PD-12. Regarding contractors, develop and maintain an accessible database containing the information outlined in Recommendation Two, as well as the contract number, similar CPSC position, contractor name, employer, and name of contracting officer's representative.
PD-13. Complete the work required to fully implement OPM's recommendations from 2017.

Audit of the CPSC's Implementation of FMFIA for FYs 2018 and 2019 (FMFIA)

May 12, 2021

FMFIA-1. Provide guidance identifying programs and/or activities as a part of its internal guidance and in accordance with achieving its mission requirements**.**
FMFIA-2. Align programs and/or activities with applicable reporting requirements.
FMFIA-3. Report programs and/or activities in accordance with applicable Federal criteria.
FMFIA-4. Provide training to CPSC program managers on how to develop and implement a formal internal controls program in accordance with Standards for Internal Control in the Federal Government, OMB Circular A-123, and CPSC policies and procedures.
FMFIA-5. Develop a formal internal controls program over operations for CPSC programs.
FMFIA-6. Evaluate staffing needs within the Office of Financial Management, Planning and Evaluation to support internal controls and FMFIA reporting requirements.
FMFIA-7. Establish formal lines of communication between the Office of Financial Management, Planning and Evaluation and CPSC program management for the purpose of assessing and monitoring internal control programs and compliance with FMFIA requirements.

Evaluation of the CPSC's FISMA Implementation for FY 2021

Transmitted: October 29, 2021

FISMA21-2. 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).
FISMA21-3. Establish and implement policies and procedures to manage software licenses using automated monitoring and expiration notifications (Risk Management ii/iii).
FISMA21-4. 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).
FISMA21-5. 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).
FISMA21-6. 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).

[3] *One recommendation from this audit is no longer monitored due to agency disagreement with the recommendation.

Reports With Open Recommendations

FISMA21-7. 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).
FISMA21-8. 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).
FISMA21-9. 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).
FISMA21-10. Develop and implement a supply chain risk management plan (Supply Chain Risk Management i).
FISMA21-11. Develop and implement an information security architecture that supports the Enterprise Architecture. (Risk Management vii).
FISMA21-12. Develop an Enterprise Architecture to be integrated into the risk management process (Risk Management vii).
FISMA21-13. 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).
FISMA21-15. Develop and implement a Configuration Management plan to ensure it includes all requisite information (Configuration Management ii/iii).
FISMA21-16. 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).
FISMA21-17. Integrate the management of secure configurations into the organizational Configuration Management process (Configuration Management v).
FISMA21-18. Consistently implement flaw remediation processes, including the remediation of critical vulnerabilities (Configuration Management vi).
FISMA21-19. Identify and document the characteristics of items that are to be placed under Configuration Management control (Configuration Management vii).
FISMA21-20. Establish measures to evaluate the implementation of changes in accordance with documented information system baselines and integrated secure configurations (Configuration Management vii).
FISMA21-21. 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).
FISMA21-22. 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).
FISMA21-23. 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)
FISMA21-24. Define and implement a process to ensure the completion of access agreements for all CPSC users. (Identity and Access Management v).
FISMA21-25. Enforce Personnel Identity Verification card usage for authenticating to all CPSC systems (Identity and Access Management vi).
FISMA21-26. Identify and document potentially incompatible duties permitted by privileged accounts (Identity and Access Management vii).
FISMA21-27. Document and implement a process to restrict the use of privileged accounts and services when performing non-privileged activities (Identity and Access Management vii).
FISMA21-29. Log and actively monitor activities performed while using privileged access that permit potentially incompatible duties (Identity and Access Management vii).
FISMA21-30. Define and implement the identification and authentication policies and procedures (Identity and Access Management ii).
FISMA21-31. Define and implement processes for provisioning, managing, and reviewing privileged accounts (Identity and Access Management vii) (2021 recommendation).
FISMA21-32. 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).
FISMA21-33. Document and implement a process for periodically reviewing for and removing unnecessary Personally Identifiable Information from agency systems (Data Protection and Privacy i).
FISMA21-35. 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).

Reports With Open Recommendations

FISMA21-36. Perform an assessment of the knowledge, skills, and abilities of CPSC personnel with significant security responsibilities (Security Training i).
FISMA21-37. 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).
FISMA21-38. 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).
FISMA21-39. Integrate the established strategy for identifying organizational risk tolerance into the Information Security Continuous Monitoring plan (Information Security Continuous Monitoring i).
FISMA21-40. 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).
FISMA21-44. 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).
FISMA21-45. 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).
FISMA21-46. Integrate documented contingency plans with the other relevant agency planning areas (Contingency Planning iii).
FISMA21-47. Test the set of documented contingency plans (Contingency Planning iv).

Evaluation of the CPSC's NIST Cybersecurity Framework Implementation

Transmitted: January 18, 2022

NIST-1. Complete a National Institute of Standards and Technology (NIST) Cybersecurity Framework current profile in accordance with NIST guidance.
NIST-2. Conduct an assessment to identify the highest risks to the CPSC's security profile based on the information learned while completing the National Institute of Standards and Technology Cybersecurity Framework current profile exercise.
NIST-3. Complete a National Institute of Standards and Technology Cybersecurity Framework (NIST) target profile in accordance with NIST guidance.
NIST-4. Perform an assessment to identify gaps between the current and target National Institute of Standards and Technology Cybersecurity Framework profiles.
NIST-5. Update and implement the CPSC Framework Implementation Action Plan.

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