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

Semiannual Report to Congress

April 1, 2021 to September 30, 2021

October 29, 2021

22-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.

MESSAGE FROM THE INSPECTOR GENERAL

I am pleased to submit the Office of Inspector General (OIG) for the U.S. Consumer Product Safety Commission's (CPSC) Semiannual Report to Congress.

This Semiannual Report details the work of the OIG in the oversight of the CPSC for the second half of Fiscal Year (FY) 2021.

As I write this, we remain in full-time telework due to the pandemic. During these extraordinary times, my professional and dedicated staff have remained focused on work that improves the CPSC's ability to achieve its mission as well as fighting fraud, waste, and abuse.

FY 2022 will bring both new challenges and opportunities for the CPSC and our office. After operating largely under emergency telework procedures throughout FY 2021, the CPSC has announced its intention to return employees to the office early in FY 2022. This will be accomplished through a pilot telework program that will allow up to four days per week of telework and require hoteling of employees who telework more than half-time.

Congress has appropriated the CPSC $50 million in pandemic related funding. The CPSC has stated its intention to utilize the funding to increase their port coverage as well as address ongoing information technology and administrative needs. It is also seeking a substantial increase in its non-pandemic funding for FYs 2022 and 2023.

The OIG has recently initiated plans to reorganize and expand our office to better provide oversight of the CPSC as it grows and evolves. We are concerned that the internal control challenges currently facing the agency may adversely impact the CPSC's utilization of the additional funding it is receiving. As detailed in our Audit of the CPSC's Implementation of the Federal Managers' Financial Integrity Act, the CPSC has not established and implemented a formal internal controls program over its operations.

Additionally, there is 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.

Finally, as discussed in greater detail on page 18, during this reporting period, the CPSC's Chief Information Officer acted to prevent OIG investigators from directly accessing agency emails, thus delaying ongoing investigations. To resume our work until the matter can be appropriately resolved, we have reluctantly agreed to a proposal made by the then acting Chairman to allow an agency information technology specialist to conduct email searches on our behalf. We have raised this issue with the new chairman and are hoping for a resolution that restores our direct access.

We look forward to the new fiscal year and the opportunities and challenges that will come with it.

Christopher W. Dentel, Inspector General

TABLE OF CONTENTS

BACKGROUND 2
U.S. Consumer Product Safety Commission 2
Office of Inspector General 2
AUDIT PROGRAM 5
Completed Reports During this Reporting Period 5
Ongoing Audit Program Activity 7
Previously Issued Reports with Open Recommendations 8
INVESTIGATIVE PROGRAM 14
OTHER ACTIVITIES 16
OIG COORDINATION 17
INSTANCES OF CPSC INTERFERENCE WITH OIG ACCESS 18
SIGNIFICANT MANAGEMENT DECISIONS WITH WHICH THE INSPECTOR GENERAL DISAGREES 19
APPENDIX A: CROSS REFERENCE TO REPORTING REQUIREMENTS OF THE IG ACT 20
APPENDIX B: PEER REVIEWS 21
APPENDIX C: STATEMENT REGARDING PLAIN WRITING 22
APPENDIX D: STATISTICAL DATA 23
APPENDIX E: STATUS OF RECOMMENDATIONS 24

BACKGROUND

U.S. Consumer Product Safety Commission

The U.S. Consumer Product Safety Commission (CPSC or Commission) 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, and the Child Nicotine Poisoning Prevention Act.

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 CPSIA, as well as numerous other laws.

By statute, the CPSC is headed by five commissioners appointed by the president 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.

The CPSC's headquarters is located in Bethesda, Maryland. The CPSC also operates the National Product Testing and Evaluation Center in nearby Rockville, Maryland and has field personnel throughout the country.

This latest semiannual period brought a number of major changes to the CPSC. First, the agency received $50 million in additional funds through the American Rescue Plan Act of 2021. These funds are to be targeted towards increased staffing at ports, additional compliance efforts, and additional information technology enhancements. Second, the president nominated three individuals to the Commission, including a permanent chairman. As of the writing of this report, the new chairman has been confirmed, one nominee awaits final confirmation by the full Senate, and one nominee awaits a committee vote. The confirmation of the new chairman marks the first time a permanent chairman has headed the CPSC since February 2017.

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.

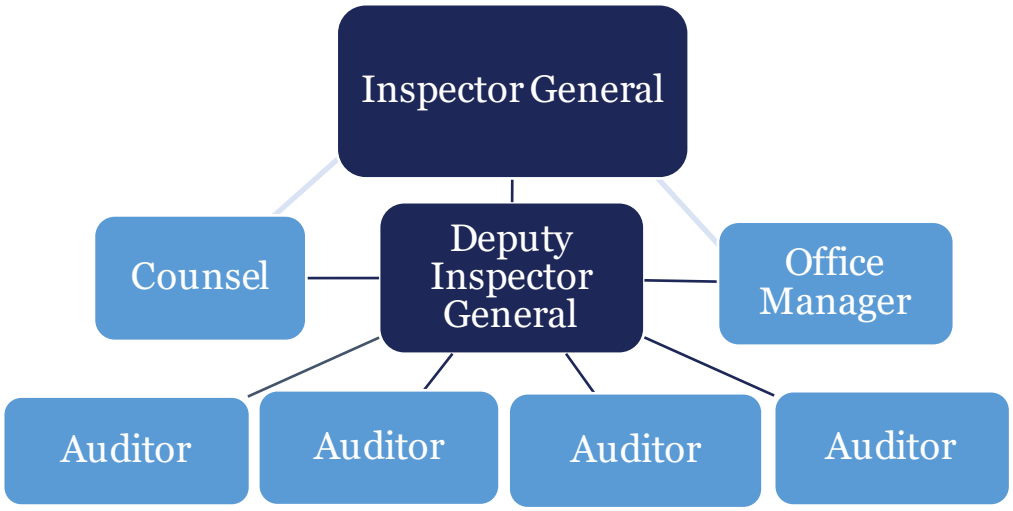
We strive to offer actionable recommendations to increase the efficiency and effectiveness of the CPSC in its mission to protect the public against unreasonable risks of injuries associated with consumer products. We focus our available resources on high-risk areas and continuously seek ways to provide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

The OIG operates from the CPSC headquarters building in Bethesda, MD. Our office is currently made up of seven employees, we plan to add an eighth and ninth employee in the next two years to provide oversight of the agency's expanding funding and operations.

Additionally, in Fiscal Year (FY) 2021 we initiated an information technology modernization project to improve the efficiency of OIG operations. This effort is ongoing, but when completed will provide the OIG with a more efficient reporting process and an audit documentation repository with enhanced functionality. This will also be the first time we will have automated investigative workpapers. Because our tool is a FedRAMP approved cloud-based system, we will have enhanced data security. This tool will also allow us to integrate audit, investigation, and office management functions for easier planning and office management.

Finally, the OIG uses an annual risk assessment process to determine which programs at the CPSC present the greatest risk to the agency and in turn, require auditing by the OIG. Based on various factors a composite score is assigned to individual programs and then tallied to make determinations whether to include the program in the following year's audit plan.

Office of Inspector General Organizational Chart



AUDIT PROGRAM

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

Completed Reports During this Reporting Period

Evaluation of the CPSC's Implementation of the Federal Data Strategy 2020 Action Plan
Transmitted: April 16, 2021
For the full report click here

The OIG contracted with Williams, Adley & Company-DC, LLP (Williams Adley) to perform a review of the CPSC's implementation of the Federal Data Strategy. The objective of this requirement was to obtain an independent evaluation of the CPSC's implementation of the Office of Management and Budget (OMB) Memorandum (M)-19-18, *Federal Data Strategy - A Framework for Consistency*, and associated OMB-issued action plans. The review was performed in accordance with Council of the Inspectors General for Integrity and Efficiency (CIGIE) Quality Standards for Inspection and Evaluation (QSIE). Williams Adley found that the CPSC completed the required agency actions described in the most recent action plan published by OMB, and made four recommendations to improve the agency's ability to leverage data as an asset and business resource 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 Process
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 Generally Accepted Government Auditing Standards (GAGAS). The audit

identified $49,631 in questioned costs. The report contained 13 recommendations to strengthen the program and all remain open. The agency did not concur with one of the recommendations.

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

The OIG contracted with Kearney and Company (Kearney) to perform an audit of the CPSC's compliance with the Federal Managers' Financial Integrity Act (FMFIA) in FYs 2018 and 2019. 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, as published in the Agency Financial Report. The review was performed in accordance with GAGAS. Kearney determined that the CPSC did not comply with FMFIA for CPSC operations for FYs 2018 and 2019. Specifically, a misalignment exists between how the CPSC identifies programmatic or operational activities, how it measures the performance of these activities, and how it reports these activities. These "operational activities" were not programs but offices within the CPSC. 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*. This audit made seven recommendations to improve the internal controls program and all remain open.

Review of the CPSC's Compliance with the Payment Integrity Information Act for Fiscal Year 2020
Transmitted**:** May 17, 2021
For the full report click here

The OIG contracted with 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 2020. The review focused on the CPSC's compliance with the six elements identified as criteria in the OMB guidance, as well as overall program internal controls. The review was performed in accordance with CIGIE QSIE. In accordance with OMB, all applicable elements must be complied with in order to result in overall compliance. Kearney found the CPSC complied with all applicable elements of PIIA for FY 2020. This report made no recommendations.

The Office of Inspector General's Survey on Employee Return to Regular Work Locations
Transmitted: May 27, 2021
For the full report click here

The goals of the survey were to identify employee concerns to help plan for the transition away from fulltime mandatory telework as the pandemic eases. The survey also collected employee views on continued communication from management about returning to work and views about preferred future work schedules and locations. This is a special project, outside the OIG work plan, and was not performed in accordance with GAGAS. This survey made no recommendations.

Independent Risk Assessment of the CPSC's Charge Card Programs
Transmitted**:** September 1, 2021
For the full report click here

The objective of this engagement was to assess risks associated with the CPSC's charge card programs in FY 2020. This review was performed in accordance with attestation standards established by the Government Accountability Office and the American Institute of Certified Public Accountants. Overall, we concluded that the risk of illegal, improper, or erroneous purchases and payments through the CPSC's charge card programs during the assessment period was medium for the purchase card and low for the travel and fleet card programs. This report made no recommendations.

Ongoing Audit Program Activity

Audit of the CPSC's FY 2021 Financial Statements
The OIG contracted with CliftonLarsonAllen, LLP (CLA), 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, 2021. 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 GAGAS.

Evaluation of the CPSC's FISMA Implementation for FY 2021
The OIG contracted with Williams Adley to perform a review of the CPSC's compliance with the reporting requirements of the Federal Information Security Modernization Act of 2014 (FISMA) for FY 2021. The objective of this review is 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's M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*. The review is being performed in accordance with CIGIE QSIE.

Evaluation of the CPSC's Implementation of the Cybersecurity Framework
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. The objective of this review is to evaluate the progress the CPSC has made toward implementing the Cybersecurity Framework and to identify cyber defense controls that require implementation or improvement. The review is being performed in accordance with CIGIE QSIE.

Audit of the CPSC's Compliance with The Digital Accountability and Transparency Act
The Digital Accountability and Transparency Act, in part, requires federal agencies to report financial and contract data in accordance with the established government-wide financial data standards on USAspending.gov. The Digital Accountability and Transparency Act also requires the Inspector General of each federal agency to review a statistically valid sample of the spending data submitted by its federal agency and to submit to Congress a publicly available report assessing the completeness, accuracy, timeliness, and quality of the data sampled and the implementation and use of the government-wide data standards by the federal agency. The scope of this audit is FY 2021, first quarter (October 1, 2020 – December 31, 2020) data. This audit is being performed in accordance with GAGAS.

Review of Human Resources Management Practices
The OIG contracted with AE Strategies (AES) to evaluate the CPSC's human resources function's ability to provide adequate support to the CPSC as the agency experiences a period of rapid growth. AES will evaluate the human resources function through three lenses: tactical agency support including completing transactional services for the CPSC; strategic agency policy support such as helping CPSC plan for future human capital needs; and management of CPSC's human resources function. This work will be performed using Office of Personnel Management assessment tools to measure effectiveness of federal human resources functions.

Previously Issued Reports with Open Recommendations

Please see Appendix E 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 (CPSRMS). 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 associated with this report and five remain open.

Opportunities Exist to Ensure CPSC Employees are Satisfying in Good Faith Their Just Financial Obligations
Transmitted: September 30, 2014
For the full report click here

The objective of this review was to determine whether the CPSC had established adequate internal controls over employee wage garnishments and appropriate tax withholdings. The OIG conducted a review of the CPSC's efforts to ensure its employees were satisfying their financial obligations in good faith, especially those related to federal, state, or local taxes. We also assessed the CPSC's compliance with identified applicable laws, regulations, and court ordered judgments. This review was conducted in accordance with CIGIE QSIE. We determined that the CPSC Office of Human Resources Management had not established proper oversight procedures over wage garnishments processed by their service provider, the Interior Business Center of the U.S. Department of the Interior. There were two consolidated recommendations associated with this report and both remain open.

Audit of the Freedom of Information Act Program
Transmitted: September 30, 2015
For the full report click here

The objective of this audit was to determine whether the CPSC had developed proper internal controls over its Freedom of Information Act (FOIA) program. This included assessing the adequacy of the policies and procedures to comply with the FOIA laws and regulations. We also examined fee assessments for FOIA requests processed between October 1, 2008, and September 30, 2013. The OIG conducted this audit under GAGAS. We found that although the CPSC had a functioning program, we identified several internal control weaknesses and noted that the program did not comply with certain policies and procedures mandated by the FOIA. There were 11 consolidated recommendations associated with this report and 7 remain open.

Cybersecurity Information Sharing Act of 2015 Review Report
Transmitted: August 14, 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 but 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 (OEP) in place for FY 2017. The purpose of an OEP 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 Programs: An Interagency Security Committee Guide* and other criteria. The audit was performed in accordance with GAGAS. Overall, we found that the CPSC's OEP 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 10 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 operating until 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 and processes Kearney made 25 recommendations and 18 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 (DPS) 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, DPS 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 14 remain open.

Audit of the CPSC's Grants Program
Transmitted: September 25, 2020
For the full report click here

The OIG audited the CPSC's Pool Safely Grants Program (PSGP) for all grants awarded prior to September 30, 2018. The objectives of this audit were to assess agency compliance with the laws and regulations that govern the PSGP, the overall effectiveness of the PSGP, the adequacy of the PSGP's internal control environment, and management's monitoring and administration of the program. The audit was performed in accordance with GAGAS. The OIG determined that the PSGP was not effective; and the audit identified $1,722,084 in questioned costs. The OIG made 22 recommendations to improve the PSGP 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. The OIG made 40 recommendations and all remain open.

Evaluation of CPSC's FISMA Implementation for FY 2020
Transmitted: November 3, 2020
For the full report click here

The OIG contracted with Williams, Adley to review the CPSC's compliance with the reporting requirements of FISMA for FY 2020. The objective of this review was to determine the effectiveness of the CPSC's information security program in accordance with the FY 2020 FISMA reporting requirements, issued by the Department of Homeland Security and OMB's M-20-04, *Fiscal Year 2019-2020 Guidance of 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 metrics. However, the CPSC was making progress in implementing many FISMA requirements. Williams Adley made 47 recommendations to improve the CPSC's information security posture. CPSC's progress in resolving these recommendations will be evaluated as part of the FY 2021 FISMA evaluation.

Review of the CPSC's NEISS Program
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 makes 12 recommendations to improve NEISS data governance and support the methodology to determine costs charged to other agencies and 10 remain open.

Audit of the CPSC's FY 2020 Financial Statements
Transmitted: November 16, 2020
For the full report click here

The OIG contracted with CLA to perform an independent audit of the CPSC's financial statements according to all current standards for the period ended September 30, 2020. The objective of this audit was to determine whether the CPSC's financial statements presented 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 was performed in accordance with GAGAS. CLA identified a significant deficiency in internal control regarding the monitoring and tracking of the amortization of leasehold improvements and automated data processing software, and a reportable violation of fiscal law. This audit makes two recommendations to improve controls over asset accounting. The CPSC's progress in resolving these recommendations will be evaluated as part of the FY 2021 financial statement audit.

Audit of the 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 while OCM met or exceeded their targeted number of communications to the public, 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 to improve data quality and reliability and all 11 remain open.

INVESTIGATIVE PROGRAM

The OIG investigates complaints and information received from CPSC 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, and waste of funds. 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 conduct 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, 2021, through September 30, 2021.

Investigation Status	Count
Open as of April 1, 2021	**6**
Opened during reporting period	38
Closed during reporting period	4
Transferred to other Departments/Agencies	35
Referred to Department of Justice for Criminal Prosecution	2
Referred for State/Local Criminal Prosecution	0
Total Indictments/Information from Prior Referrals	0
Open as of September 30, 2021	**5**

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

Reportable Investigations

21-63 Complaint alleged waste in the administration of a compliance program. The complaint is currently under investigation. This investigation is delayed due to ongoing issues related to access to information.

21-70 Complaint alleged a senior government official had improperly shared confidential information on social media. This complaint was a follow-on to complaint 21-25 (from the previous reporting period). In all, the OIG investigated five out of the six allegations raised. The OIG determined one allegation should be investigated by the Office Human Resources Management in accordance with the agency's anti-harassment policy. All five allegations from the two complaints investigated by the OIG were referred to the Department of Justice. The Department of Justice declined to accept any of the allegations for criminal prosecution. After

conducting two thorough administrative inquiries involving the interviewing of more than 35 people, the OIG determined there was insufficient evidence to substantiate the allegations. Both complaints investigated by the OIG are now closed.

21-82 Complaint alleged coercion and conflict of interest related to the regulation of a consumer product. 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:

Administrative False Claims Act
Anti-Deficiency Act
Consumer Product Safety Act
Consumer Product Safety Commission Regulations
Consumer Product Safety Improvement Act of 2008
Coronavirus Aid, Relief, and Economic Security Act (2020)
Consolidated Appropriations Act, 2021
Economy Act
Ethics Regulations
Executive Order on Diversity, Equity, Inclusion, and Accessibility in the Federal Workforce
Executive Order on Requiring Coronavirus Disease 2019 Vaccination for Federal Employees
Families First Coronavirus Response Act
Federal Acquisition Regulations
Federal Sector Equal Employment Opportunity Complaint Processing Regulations
Freedom of Information Act
Geospatial Act
Hatch Act
American Rescue Plan Act of 2021
Inspector General Act of 1978, as amended
Office of Management and Budget Circulars and Memoranda
Payment Integrity Information Act
Public Disclosure of Information, 15 U.S.C. 2055
Privacy Program
Prohibited Personnel Practices
Records Management Policies and Regulations
Standards of Conduct for Government Employees
Uniform Grant Guidance
Virginia Graeme Baker Pool and Spa Safety Act
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 Legislation as well as Inspection and Evaluation Committees 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 U.S. 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. The Council 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.

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 (the CPSC) to interfere with the independence of the CPSC 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 has encountered a situation where the agency interfered with OIG 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 CIO's proposal was to have EXIT staff conduct searches relating to OIG investigations and required 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. However, the Office of General Counsel (OGC), which had the same access to agency email as OIG previously enjoyed, appears to be maintaining the access now being denied OIG. OGC has hired contractors to conduct e-discovery and they appear to have continued unfettered access to agency email.

This issue was raised to Acting Chairman Adler and still has not been fully resolved, causing our investigations to be delayed and oversight to be affected. To allow our office to resume its work until the matter can be appropriately resolved, we have 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.

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 Audit of the CPSC's Position Designation and Suitability Program made thirteen recommendations; the CPSC disagreed with number 8: Establish a process to include Office of Human Resources Management during the drafting of the statement of work to determine the appropriate investigative tier for contractors prior to when the request for quotes is released to potential vendors.

Office of Human Resources Management maintained that there is no need to disclose this information to a contractor. However, there have been multiple instances of a contractor not realizing they needed to supply individuals that can pass certain background checks. Time and money are wasted while trying to onboard contractors only to realize they lack the credentials to work on a project. A simple disclosure could remedy this inefficiency. The Inspector General disagrees with this type of waste.

APPENDIX A: CROSS REFERENCE TO REPORTING REQUIREMENTS OF THE IG ACT

Citation	Reporting Requirements	Page(s)
Section 4(a)(2)	Review of legislation and regulations.	16
Section 5(a)(1)	Significant problems, abuses, and deficiencies.	5-8
Section 5(a)(2)	Recommendations with respect to significant problems, abuses, and deficiencies.	5-8
Section 5(a)(3)	Prior significant recommendations on which corrective action has not been completed.	8-13, 24-31
Section 5(a)(4)	Summary of matters referred to prosecutorial authorities and results.	14
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.	5-6
Section 5(a)(7)	Summary of each particularly significant report.	5-8
Section 5(a)(8)	Table showing the number of audit, inspection, and evaluation reports and dollar value of questioned costs for reports.	23
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 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.	8-13, 24-31
Section 5(a)(11)	Significant revised management decisions.	NA
Section 5(a)(12)	Significant management decisions with which the IG disagrees.	19
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.	21
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.	21
Section 5(a)(17)	Statistical table showing total number of investigative reports, referrals, and results of referrals.	14
Section 5(a)(18)	Metrics used to develop data for table in section 5(a) (17).	14
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.	18
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 through contractors.

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 Office of Inspector General. We gave United States International Trade Commission OIG an External Peer Review rating of pass. No deficiencies were noted and no formal recommendations were made in that review.

Inspection and Evaluation (I&E) 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 I&E organization and opined that our internal policies and procedures for the period ending June 30, 2020, are 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 OIG led a peer review team on December 16, 2019, to review the Office of Personnel Management Office of Inspector General I&E Organization. We opined that their policies and procedures and work done for the period ending June 30, 2019, were current and consistent with the covered CIGIE QSIE standards.

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	
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CLA	CliftonLarsonAllen, LLP
CPSA	Consumer Product Safety Act
CPSIA	Consumer Product Safety Improvement Act of 2008
CPSC and Commission	U.S. Consumer Product Safety Commission
DPS	Defense Point Security
EEO	Equal Employment Opportunity
FISMA	Federal Information Security Modernization Act of 2014
FOIA	Freedom of Information Act
FMFIA	Federal Managers' Financial Integrity Act
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
I&E	Inspection and Evaluation
IG Act	The Inspector General Act of 1978, as amended
Kearney	Kearney & Company
M	Memorandum
NEISS	National Electronic Injury Surveillance System
OCM	Office of Communications Management
OEP	Occupant Emergency Program
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIIA	Payment Integrity Information Act
PSGP	Pool Safely Grants Program
QSIE	Quality Standards for Inspection and Evaluation
Williams Adley	Williams, Adley & Company-DC, LLP

APPENDIX D: STATISTICAL DATA

	Number of Audit Reports	Total Questioned Costs	Total Unsupported Costs
Management decisions pending, beginning of reporting period	0	$0.00	$0.00
Issued during period	1	$49,631.00	$0.00
Needing management decision during period	1	$49,631.00	$0.00
Management Decision Made During Period			
Amounts agreed to by management	1	$49,631.00	$0.00
Amounts not agreed to by management	0	$0.00	$0.00
No Management Decision Made During Period			
Less than 6 months old	0	$0.00	$0.00
More than 6 months old	0	$0.00	$0.00

APPENDIX E: STATUS OF RECOMMENDATIONS

During this most recent reporting period, management closed 15 recommendations, most made relatively recently. As reported previously, the CPSC's closure rate has been in decline resulting in open recommendations that are nearly 10 years old. During this most recent semiannual period, the OIG made an additional 28 recommendations which are not yet reflected in the table while the agency closed 15. For a comparison, in the prior six months the CPSC closed 5 recommendations while the OIG made an additional 23 recommendations. This table provides a summary of reports with open recommendations more than six months old as of the end of the semiannual period and shows progress made closing recommendations during the last six months.

Summary of Recommendation Implementation Progress

Report Short Title	Report Date	Total Recommendations	Closed prior to April 1, 2021	Open as of April 1, 2021	Closed during the period	Open as of September 30, 2021	Total Days Past Due
RMS	6/5/2012	8	3	5	0	5	3224
Debt	9/30/2014	2	0	2	0	2	2377
FOIA	9/30/2015	11	4	7	0	7	2012
Cybersecurity	8/14/2016	5	0	5	0	5	1693
Contracts	7/25/2017	14	13	1	1	0	0
Telework	9/29/2017	9	4	5	0	5	1282
OEP	6/7/2018	12	2	10	0	10	1031
Directives	3/21/2019	2	1	1	0	1	744
Property	5/31/2019	25	7	18	0	18	673
Pentest	6/11/2019	40	25	15	1	14	662
Grants	9/25/2020	22	0	22	11	11	190
Breach	9/25/2020	40	0	40	0	40	190
NEISS	11/9/2020	12	0	12	2	10	145
OCM	2/19/2021	11	0	11	0	11	43
		213	**59**	**154**	**14**	**140**	

The table below shows all open recommendations as of the end of the current semiannual period.

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.

Opportunities Exist to Ensure CPSC Employees Are Satisfying in Good Faith Their Just Financial Obligations (Debt)

September 30, 2014

Debt-1. Management develops and documents an internal process to effectively and actively monitor employee wage garnishments pursuant to a lawful court order and transferred from the Department of the Treasury's Treasury Offset Program.
Debt-2. Management develops a process to regularly, at least annually, review employee exemption and withholding status for reasonableness.

Audit of the Freedom of Information Act Program (FOIA)

September 30, 2015

FOIA-1. Revise and implement the CPSC FOIA Program directive and related appendices to ensure consistency with current legal requirements established by the FOIA to include document retention, training, fee assessment requirements, program monitoring, revenue reconciliation, timely updating of the public reading room.
FOIA–3. Management develops SOP consistent with current FOIA legislation related to receipt, processing, and tracking of FOIA requests for IDI files.
FOIA–5. Management develops a record retention schedule that complies with all current document retention requirements.
FOIA–6. Management develops an effective FOIA monitoring system to measure timeliness of completion of all FOIA requests within statutory deadlines whether they should be assessed fees.
FOIA–8. Develop and utilize guidance to determine subject(s) of frequent requests in the "reading room" and perform timely updates to reflect frequent requests.
FOIA–10. Management develops standard operating procedures to provide guidance on compiling the annual report to the DOJ to include a documented supervisory review and sign-off.
FOIA–11. Management documents a review of the data fields in FOIAXpress for accuracy, completeness, and timeliness.

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.

The table below shows all open recommendations as of the end of the current semiannual period.

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-3. Develop and implement an effective communication strategy to include ongoing awareness and general information for all facility occupants about the OEP and expectations.
OEP-4. Develop and implement policies employing multiple communication channels for notifying staff during drills and emergency situations.
OEP-5. Develop and implement occupant accountability procedures to be practiced during drills and used during emergencies.
OEP-6. Develop and implement an effective OEP team training program with drills and exercises to include all team members at least annually.
OEP-7. Develop and implement a corrective action process that reviews the results of all drills, exercises, and actual emergencies and documents whether to update OEP guidance, including showing the updated guidance.
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. Update directives to ensure they align with directives system policies and procedures as well as reflect the current CPSC organizational structure and operations.

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.

The table below shows all open recommendations as of the end of the current semiannual period.

PMS-17. Develop, approve, and implement procedures to ensure that standard users and administrators are included in the periodic review of PMS user access and that the custodian user access is validated appropriately when performing the review.
PMS-18. Update the PMS Internal Control Document, or equivalent documentation, to reflect PMS's updated process.
PMS-19. Complete and document the periodic review for all PMS users in accordance with PMS's updated procedures.
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 (PT)

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-32. REDACTED
PT-35. REDACTED
PT-36. REDACTED
PT-38. REDACTED
PT-39. REDACTED

AUDIT OF THE CPSC'S GRANTS PROGRAM (Grants)

September 25, 2020

GRANTS–1. Implement and document awardee reporting requirements based on the results of the financial risk assessments.
GRANTS-4. Ensure that the CPSC require awardees measure performance against outcomes as well as specific objectives.
GRANTS-6. Complete and implement grant monitoring policies and procedures which include prior notice and approval requirements for grant changes that are in accordance with Uniform Guidance.
GRANTS–8. Require invoices which include the dates goods and services are provided for all awards in order to substantiate that all costs were allowable and incurred within the award's Period of Performance.
GRANTS–9. Establish a process to require timely and complete reporting from Pool Safely Grant Program awardees. Such a process may include withholding the final award remittance until after all required reports are submitted.
GRANTS-11. Obtain a written opinion from Office of General Counsel staff on the appropriateness of using VGB Act grant funds to pay for swimming lessons, whether such use violated the Purpose Act and, if a violation of the Purpose Act occurred, whether or not this violation constitutes an Anti-Deficiency Act violation.
GRANTS-14. Include specific grants governance responsibilities in all position descriptions and performance plans for persons with a role in the Pool Safely Grants Program.
GRANTS-17. Provide training on the updated Management Information System Guide to those who are likely to charge their time to VGB Act codes.
GRANTS-19. Determine what grant costs qualify as administrative costs and charge them VGB Act funds.
GRANTS-21. Ensure previous costs related to section 1405 of the VGB Act are charged to the correct appropriation.
GRANTS–22. Have Office of General Counsel provide a written determination of whether there are any Purpose Act or Anti-Deficiency Act violations related to any of the VGB Act administrative expenditures.

The table below shows all open recommendations as of the end of the current semiannual period.

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-7. Develop and document a comprehensive crisis communication plan. This plan should include a process to ensure that there is an authoritative source for data related to any incident.

BREACH-8. The crisis communication plan should include annual tabletop exercises and annual plan reviews.

BREACH-9. The CPSC should document the results of each crisis communication plan annual tabletop exercise.

BREACH-10. The CPSC should publish the resulting comprehensive crisis communication plan after any update.

BREACH-11. Develop a process to ensure that all information reported to Congress and otherwise publicly reported is reviewed for accuracy and correctly contextualized and described.

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-16. Include successful implementation of OIG recommendations as a performance metric for Senior Executive Service employees and other senior management officials.

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-20. Create a searchable online public database with scrubbed Clearinghouse data to reduce the number of individual Clearinghouse information requests that are processed.

BREACH-21. Require training for all Clearinghouse staff, up to and including the AED for EPHA, on the use and functionality of this new tool, procedures for responding to requests for information, and requirements to protect 6(b) information and PII data. Include this training as part of the onboarding for all Clearinghouse staff, up to and including the AED for EPHA.

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-28. Use the data from the tracking system to develop and publish annual statistics related to the work of the Clearinghouse.

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.

The table below shows all open recommendations as of the end of the current semiannual period.

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-31. Develop, implement, and require participation by all senior EXHR management staff in a training program on the values and benefits of an internal control system including a session on the statements of assurance process and its importance.
BREACH-32. Determine, document, and implement a structure for the Clearinghouse.
BREACH-33. Determine, document, and implement the role of the Freedom of Information Act Office in responding to Clearinghouse requests.
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-36. Complete and document the results of a risk assessment of Clearinghouse operations.
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-39. Ensure that activities fulfilling Clearinghouse data requests be made visible to management through the creation and use of a specific WebTA code based on a newly created Management Information System code.
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.

Evaluation of CPSC's FISMA Implementation for FY 2020[1] (FISMA20)
November 3, 2021

FISMA20-1. Develop and implement a process to maintain an up-to-date and complete information system inventory (2020 recommendation).
FISMA20-2. Develop, document, and implement a process for determining and defining system boundaries in accordance with National Institute of Standards and Technology guidance (prior year recommendation).
FISMA20-3. Establish and implement a policy and procedures to manage software licenses using automated monitoring and expiration notifications (prior year recommendation).
FISMA20-4. REDACTED (prior year recommendation).
FISMA20-5. Define and document the taxonomy of CPSC's information system components, and classify each information system component as, at minimum, one of the following types: IT system (e.g., proprietary and/or owned by the CPSC), application (e.g., commercial off-the-shelf, government off-the-shelf, or custom software), laptops and/or personal computers, service (e.g., external services that support CPSC's operational mission, facility, or social media) (prior year recommendation).
FISMA20-6. Identify and [REDACTED] that establishes set policies for hardware and software access on the agency's network (prior year recommendation).
FISMA20-7. Develop and implement a formal strategy to address information security risk management requirements as prescribed by the National Institute of Standards and Technology guidance (prior year recommendation - modified).
FISMA20-8. Complete an assessment of information security risks related to the identified deficiencies and document a corresponding priority listing to address identified information security deficiencies and their associated recommendations. A corrective action plan should be developed that documents the priorities and timing requirements to address these deficiencies (prior year recommendation - modified).
FISMA20-9. Develop and implement an Enterprise Risk Management (ERM) program based on National Institute of Standards and Technology and ERM Playbook (A-123, Section II requirement) guidance. This includes establishing a cross-departmental risk executive (function) lead by senior management to provide both a departmental and organization level view of risk to the top decision makers within the CPSC (prior year recommendation).
FISMA20-10. Develop and implement a supply chain risk management plan (prior year recommendation).
FISMA20-11. Develop and implement an information security architecture that supports the CPSC Enterprise Architecture and is integrated into the agency's Enterprise Risk Management Program (2020 recommendation).
FISMA20-12. Develop an Enterprise Architecture to be integrated into the risk management process (prior year recommendation).
FISMA20-13. Establish and implement policies and procedures to require coordination between the Office of Information Technology and the Office of Procurement to facilitate identification and incorporation of the appropriate clauses within all contracts (prior year recommendation).
FISMA20-14. Further define the resource designations for a Change Control Board (prior year recommendation).
FISMA20-15. Develop and implement a Configuration Management plan to ensure it includes all requisite information (prior year recommendation).
FISMA20-16. Develop, implement, and disseminate a set of Configuration Management (CM) procedures in accordance with the inherited CM Policy [REDACTED] (prior year recommendation).

[1]As a reflection of the changing FISMA metrics, this table includes only recommendations from the most recent FISMA report.

The table below shows all open recommendations as of the end of the current semiannual period.

FISMA20-17. REDACTED (prior year recommendation).
FISMA20-18. Identify and document the characteristics of items that are to be placed under Configuration Management control (prior year recommendation).
FISMA20-19. Establish measures to evaluate the implementation of changes in accordance with documented information system baselines and integrated secure configurations (prior year recommendation).
FISMA20-20. Consistently implement[REDACTED], including the remediation of [REDACTED] (2020 recommendation).
FISMA20-21. Define and document all the critical capabilities that the CPSC manages internally as part of the Trusted Internet Connection (TIC) program (prior year recommendation).
FISMA20-22. Define and document a strategy (including specific milestones) to implement Federal Identity, Credential, and Access Management (prior year recommendation).
FISMA20-23. Integrate Identity, Credential, and Access Management strategy and activities into the Enterprise Architecture and Information System Continuous Monitoring (prior year recommendation).
FISMA20-24. Develop, formalize (through the CPSC's D-100 process), and implement processes to ensure all personnel are assigned risk designations and appropriately screened prior to being granted access to agency systems. Prior to formalizing the existing risk designation procedures, these procedures should be enhanced to include the following requirements: Performance of periodic reviews of risk designations at least annually, Explicit position screening criteria for information security role appointments, Description of how cybersecurity is integrated into human resources practices (prior year recommendation).
FISMA20-25. Develop and implement a process to ensure the completion of access agreements for all CPSC information system users (2020 recommendation).
FISMA20-26. Enforce Personal Identity Verification card usage for authenticating to all CPSC systems (prior year recommendation).
FISMA20-27. Identify and document potentially incompatible duties permitted by [REDACTED] (prior year recommendation).
FISMA20-28. REDACTED (prior year recommendation).
FISMA20-29. Fully deploy the CPSC's [REDACTED] (prior year recommendation).
FISMA20-30. REDACTED (prior year recommendation).
FISMA20-31. Define and implement the identification and authentication policies and procedures (prior year recommendation).
FISMA20-32. Automatically revoke temporary and emergency access after a specified period of time (prior year recommendation).
FISMA20-33. Document and implement a process for inventorying and securing systems that contain Personally Identifiable Information or other sensitive agency data (e.g., proprietary information) (prior year recommendation).
FISMA20-34. Document and implement a process for periodically reviewing for and removing unnecessary Personally Identifiable Information from agency systems (prior year recommendation).
FISMA20-35. Develop and implement data encryption policies and procedures (2020 recommendation).
FISMA20-36. REDACTED (prior year recommendation).
FISMA20-37. Perform an assessment of the knowledge, skills, and abilities of CPSC personnel with significant security responsibilities (prior year recommendation).
FISMA20-38. Identify all CPSC personnel that affect security and privacy (e.g., Executive Risk Council, Freedom of Information Act personnel, etc.) and ensure the training policies are modified to require these individuals to participate in role-based security/privacy training (prior year recommendation).
FISMA20-39. Develop and tailor security training content for all CPSC personnel with significant security responsibilities, and provide this training to the appropriate individuals (prior year recommendation).
FISMA20-40. Integrate the established strategy for identifying organizational risk tolerance into the Information System Continuous Monitoring plan (prior year recommendation).
FISMA20-41. Define and implement Information System Configuration Management (ISCM) procedures, to include the monitoring of performance measures, that support the updates ISCM plan (2020 recommendation).
FISMA20-42. Update and implement the CPSC Incident Response (IR) policy and IR plan with latest practices, including IR performance measurers and the latest implemented network profiling techniques (2020 recommendation).
FISMA20-43. Define and implement a process to ensure the timely resolution of incidents. For example, establish routine status reviews for tracking incident response activities to completeness (prior year recommendation).
FISMA20-44. Develop and document a robust and formal approach to contingency planning for agency systems and processes using the appropriate guidance [ex. National Institute of Standards and Technology (NIST) Special Publication 800-34/53, Federal Continuity Directive 1, NIST Cybersecurity Framework, and National Archive and Records Administration guidance] (prior year recommendation).
FISMA20-45. Develop, document, and distribute all required Contingency Planning documents (ex. organization-wide Continuity of Operation Plan and Business Impact Assessment, Disaster Recovery Plan, Business Continuity Plans, and Information System Contingency Plans) in accordance with appropriate federal and best practice guidance (prior year recommendation).
FISMA20-46. Integrate documented contingency plans with the other relevant agency planning areas (prior year recommendation).
FISMA20-47. Test the set of documented contingency plans (prior year recommendation).

The table below shows all open recommendations as of the end of the current semiannual period.

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

November 9, 2020

NEISS-2. Obtain a legal opinion to determine whether the CPSC is legally allowed to perform work or obtain supplies and services in support of the NEISS Expansion program and outside of its jurisdiction.

NEISS-3. Report to the OIG as to whether an Anti-Deficiency Act violation occurred.

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-7. Develop a data governance framework to ensure that data is managed appropriately and in accordance with programmatic and regulatory requirements.

NEISS-8. Provide training to medical coders on inputting data and evaluating the accuracy of the data without making assumptions as to the product or any other data that is not presented within the medical file.

NEISS-10. Develop policies and procedures to effectively support managing automated data and quality assurance protocols, to include ensuring that errors are appropriately remediated.

NEISS-11. Update and provide training on a routine basis, preferably annually, to address issues found in data entry since the last training.

NEISS-12. Perform and provide a report to the Executive Director on an analysis of alternatives to determine if it is more cost effective for the CPSC to perform additional upgrades to the NEISS or switch to a more robust platform to provide user-centric design, better up-front preventative controls, and real-time oversight, while also incorporating emerging technologies, such as artificial intelligence that is consistent with the CPSC's desire to increase the use of quality data for better decision support.

Audit of the Consumer Product Safety Commission's Fiscal Year 2020 Financial Statements[2] (FSA)

November 15, 2021

FSA20-1. Strengthen their quality control review over the excel-based leasehold improvements and ADP software schedules.

FSA20-2. Consider transitioning from an excel-based schedule to another software/platform or enhance excel capabilities such as adding formulas to calculate number of months in service, locking formulas to avoid overriding with incorrect data input, and restricting cells to limit data input that are required to help prevent errors.

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

February 19, 2021

OCM-1. Communicate with staff on the relationship between the strategic goals and the day-to-day processes in place to achieve those goals. This communication should include discussion of the strategic goals process end- to-end.

OCM-2. Fully document and implement procedures for the process of discontinuing key performance measures, the reason for discontinuation, and intentions concerning future key performance measures.

OCM-3. Fully document and implement procedures covering the processes related to performing the activities necessary to achieve OCM's key performance measure targets.

OCM-4. Update the CPSC policies as necessary to reflect any new procedures.

OCM-5. Develop and implement procedures to maintain, retain, and update OCM program documents, at least annually.

OCM-6. Fully document and implement procedures for compiling, calculating, and reporting data in the Annual Performance Report.

OCM-7. Coordinate with the Office of Budget, Planning, and Evaluation to develop control activities to improve data confidentiality, integrity, availability, and reporting. Specifically, develop and utilize a reporting tool which includes adequate data security, or leverage the data security features that already exist in Excel. Create or incorporate into existing standard operating procedures the control activities that were developed.

OCM-8. Create and or enhance policies and procedures to include an adequate review of the spreadsheets.

OCM-9. Continue planned efforts to identify and implement tools to improve message usefulness and measure message effectiveness.

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

OCM-11. Review, at least annually, data from communication effectiveness tools, and adjust communication strategies based on the data analysis.

[2]Due to the FSA occurring annually, this table includes only includes recommendations from the most recent FSA report.

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