Office of Inspector General

U.S. Consumer Product Safety Commission

Semiannual Report to Congress

April 1, 2020 – September 30, 2020

October 30, 2020

Report 21-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.

October 30, 2020

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

FROM: Christopher W. Dentel, Inspector General

SUBJECT: Transmittal of Semiannual Report

I am pleased to present this Semiannual Report summarizing the activities of our office for the period April 1, 2020, through September 30, 2020. The U.S. Consumer Product Safety Commission (CPSC or Commission) Office of Inspector General (OIG) remains committed to promoting the economy, efficiency, and effectiveness of the CPSC's programs and operations. Our audits, investigations, and other activities highlighted in this report demonstrate this ongoing commitment.

Our audit and investigative work reflects our commitment to keep Congress, the Commission, and the public fully and currently informed of our findings and recommendations regarding CPSC programs and operations in a way that is transparent to both our internal and external stakeholders. I commend and thank my hardworking team for their efforts and dedication to our important mission. I also want to thank the Commission and the CPSC's staff for their ongoing support of our office.

In addition to our work with the CPSC, the OIG continues to be involved with the Council of the Inspectors General on Integrity and Efficiency and the Council of Counsels to the Inspectors General on issues of interest to the entire OIG community.

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, under the provisions of the Consumer Product Safety Act (Public Law 92-573), to protect the public against unreasonable risks of injuries associated with consumer products. 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 Consumer Product Safety Act and the Consumer Product Safety Improvement Act of 2008. The CPSC also regulates products covered by the Virginia Graeme Baker Pool and Spa Safety Act, the Children's Gasoline Burn Prevention Act, the Flammable Fabrics Act, the Federal Hazardous Substances Act, the Poison Prevention Packaging Act, and the Refrigerator Safety Act.

By statute, the CPSC is headed by five Commissioners appointed by the President with the advice and consent of the Senate. The Chairman of the CPSC is designated by the President as the principal executive officer of the Commission.

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

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. Dentel was named Inspector General in 2004.

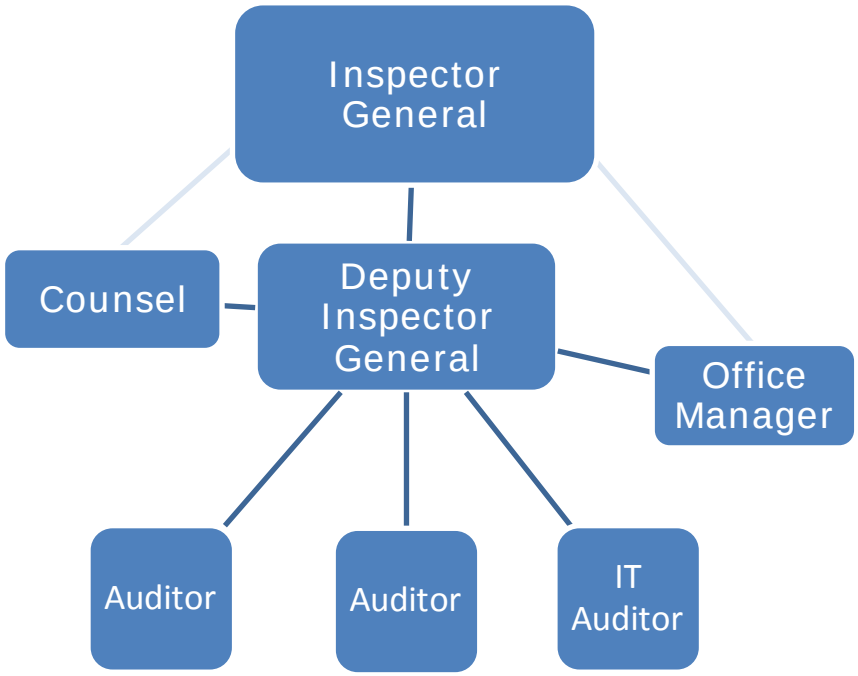
The IG Act was amended by the Inspector General Empowerment Act of 2016. The Inspector General Empowerment Act safeguards OIG access to agency information and mandates additional reporting to increase transparency in government operations.

The IG Act gives the Inspector General the authority and responsibility to:

- conduct and supervise audits and investigations of the CPSC's programs and operations
- provide leadership, coordination, and recommend policies for activities designed to promote economy, efficiency, and effectiveness in the administration of the CPSC's programs and operations
- prevent and detect fraud, waste, and abuse of the CPSC's programs and operations
- keep the Commissioners and the Congress fully and currently informed about problems and deficiencies relating to the administration of the CPSC's programs and operations and the need for progress or corrective action

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.

Office of Inspector General



Audit Program

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

Completed Reports

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 PSGP provides awardees assistance to improve pool and spa safety through the use of anti-entrapment devices and to encourage State adoption of minimum mandatory swimming pool and spa safety laws. 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 OIG determined that the PSGP was not effective and the audit identified $1,722,084 in questioned costs.[1] The audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS). The OIG made 22 recommendations to improve the PSGP.

REVIEW OF THE CPSC'S COMPLIANCE WITH IPERA FOR FY 2019
Transmitted: May 7, 2020
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 Improper Payments Elimination and Recovery Act (IPERA), as amended by the Improper Payments Elimination and Recovery Improvement Act of 2012, for transactions in fiscal year (FY) 2019. 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

[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.

CPSC's compliance with the six elements identified as criteria in the Office of Management and Budget (OMB) Memorandum (M)-18-20 for payment accuracy, as well as overall program internal controls.

Overall, Kearney found that for FY 2019, the CPSC complied with IPERA. In accordance with OMB, all elements must be complied with in order to result in overall compliance.

Ongoing Projects

AUDIT OF THE CPSC'S FY 2020 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, 2020. 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.

AUDIT OF THE CPSC'S POSITION DESIGNATION PROCESS

The OIG is auditing 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 are to determine whether all positions in the CPSC are appropriately designated and whether all CPSC employees and contractors have the appropriate background investigation completed. The audit is being performed in accordance with GAGAS.

REVIEW OF THE CPSC's NEISS PROGRAM

The OIG has 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

objectives of this review are to determine whether the CPSC has policies and procedures in place to effectively evaluate NEISS data quality and provide adequate oversight to NEISS coordinators. Specifically, to assess how the CPSC verifies data quality in NEISS reports with respect to the dimensions of accuracy, validity, consistency, completeness, timeliness, and the fulfillment of user needs. Kearney will review NEISS data from July 1, 2013 – June 30, 2019, and related policies and procedures. The review is being conducted in accordance with CIGIE QSIE.

AUDIT OF THE OFFICE OF COMMUNICATIONS MANAGEMENT'S STRATEGIC GOALS

The OIG is auditing the CPSC's Office of Communications Management's (OCM) strategic goals for FYs 2018 and 2019. The objectives of the audit are 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 will assess OCM's internal controls over the dissemination of consumer product safety information and collaboration with stakeholders. The audit is being conducted in accordance with GAGAS.

EVALUATION OF CPSC'S FISMA IMPLEMENTATION FOR FY 2020

The OIG contracted with Williams, Adley & Company-DC, LLP (Williams Adley) to perform a review of the CPSC's compliance with the reporting requirements of the Federal Information Security Modernization Act (FISMA) for FY 2020. The objective of this review is 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 M-20-04. The review is being performed in accordance with CIGIE QSIE.

AUDIT OF CPSC'S IMPLEMENTATION OF FMFIA FOR FY 2018 AND 2019

The OIG contracted with Kearney to perform an audit of the CPSC's FY 2018 and 2019 compliance with the Federal Managers' Financial Integrity Act (FMFIA) and to evaluate the effectiveness of the CPSC's process to assess internal control over program operations, as reported in the Chairman's Management Assurance Statement, as published in the Agency Financial Report. The audit is being conducted in accordance with GAGAS.

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). The Consumer Product Safety Improvement Act of 2008 requires the CPSC to implement a publicly accessible and searchable database of consumer product incident reports called CPSRMS. The period of the review was December 2010 through February 2011 and 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 CPSRMS. 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 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. This review was conducted under CIGIE QSIE. We also assessed the CPSC's compliance with identified applicable laws, regulations, and court ordered judgments. 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. The OIG completed this work in accordance with CIGIE QSIE. During this review, we also considered whether standards for logical access were appropriate. 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.

REPORT ON THE PERFORMANCE AUDIT OF INTERNAL CONTROLS OVER CONTRACT MANAGEMENT AND ADMINISTRATION FOR FISCAL YEAR 2016
Transmitted: July 25, 2017
For the full report click here

The objective of this audit was to ascertain whether the CPSC had established and implemented effective internal controls to guide its contract and acquisitions management process for its firm-fixed-price contracts and whether the contract monitoring process utilized by the CPSC adhered to applicable federal laws and regulations. The OIG contracted with Kearney to complete this audit in accordance with GAGAS. They made 14 recommendations to improve CPSC contract management and 1 remains 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 objective of this audit was to determine program effectiveness and compliance with the 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. The objective of this audit was to determine whether the CPSC's policies and procedures for the Directives System comply with federal regulations and procedures and are effective in helping agency staff meet the CPSC's mission. This audit was performed in accordance with GAGAS and focused on management of the CPSC Directives System prior to March 31, 2018.

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 of this review 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 22 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), a management consulting firm, 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 was not adequately secure. To improve the CPSC's information technology infrastructure DPS made 40 recommendations and 16 remain open.

AUDIT OF THE CPSC'S FINANCIAL STATEMENTS for FY 2019
Transmitted: November 19, 2019
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, 2019.

In CLA's opinion, the financial statements present fairly, in all material respects, the financial position, net cost, changes in net position, budgetary resources, and custodial activity of the CPSC as of, and for the years ending September 30, 2019 and 2018, in conformity with generally accepted accounting principles. However, CLA found that the CPSC did not have a robust system of internal controls regarding leases. The lease files were incomplete in the Office of Finance because there was no formal system requiring Office of Facilities staff to provide Office of Finance staff with lease information. This lack of communication resulted in the Office of Finance not having all of the information necessary to manage CPSC leases and related transactions from a financial perspective. The communication breakdown prevented personnel from performing key roles in achieving objectives in financial reporting. Finally, the monitoring activities in this area were insufficient to identify potential errors.

CLA made three recommendations to address these issues and CPSC's progress in resolving these recommendations will be reported on as part of the FY 2020 Financial Statement Audit.

Investigative Program

The OIG investigates complaints and information received from 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, 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, 2020 through September 30, 2020.

Investigation Status	Count
Open as of April 1, 2020	**6**
Opened during reporting period	44
Closed during reporting period	5
Transferred to other Departments/Agencies	42
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, 2020	**3**

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

Reportable Investigations

Complaint 19-11/Report 20-ROI-01 On April 1, 2019, the CPSC learned that a data breach involving the Clearinghouse had occurred. We agreed to assess the scope, root causes, and the CPSC's response to the data breach. We were also asked to investigate several specific allegations of misconduct.

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 lack 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 report of investigation contains 13 findings and 40 recommendations. When completed, these recommendations will significantly strengthen CPSC operations and better secure sensitive information within the Clearinghouse and across the agency as a whole.

20-32 Complaint alleged a company selling and donating bicycle helmets subject to recall. This is outside of OIG jurisdiction and was referred to agency management.

20-33 Complaint alleged a malfunctioning thermometer. This is outside of OIG jurisdiction and was referred to agency management.

20-34 Complaint alleged issues regarding lids on a food processing device. This is outside of OIG jurisdiction and was referred to agency management.

20-35 Complainant alleged retaliation on the job at an assisted living center. This is outside of OIG jurisdiction and complainant was referred to the appropriate local and state agencies.

20-36 Complaint alleged issues regarding air quality and safety in a rental unit. This is outside of OIG jurisdiction and was referred the appropriate state and federal agencies.

20-37 Complainant alleged dangerous work conditions. OIG closed this case due to lack of complainant response.

20-38 Complainant alleged being fired from a job without a board meeting. OIG closed this case due to lack of complainant response.

20-39 Complaint alleged issues regarding lack of fire safety training in restaurants on installed fire suppression devices. This is outside of OIG jurisdiction and was referred to agency management and the appropriate federal agency.

20-40 Complaint alleged workplace retaliation at a private company. This is outside of OIG jurisdiction and was referred to the company's human resources office and the appropriate state agency.

20-41 Complainant alleged denial of ECA COVID-19 benefits from federal agency due to discrimination. This is outside of our OIG jurisdiction and the complainant was referred to the appropriate federal OIG.

20-42 Complaint was mistakenly sent to our OIG instead of the appropriate federal OIG. This is outside of our OIG jurisdiction and was referred to the appropriate federal OIG.

20-43 Complaint alleged wrongful termination after refusing to complete fraudulent paperwork. The company receives federal money and is a head start program. This is outside of our OIG jurisdiction and was referred to the appropriate federal OIG.

20-44 Complaint alleged issues regarding a trailer with recalled side rails. Complainant wrote to a company for replacement side rails and has not received them. This is outside of OIG jurisdiction and was referred to agency management.

20-45 Complaint alleged workplace retaliation and an assault at a military base. This is outside of our OIG jurisdiction and was referred to the appropriate local and federal agencies.

20-46 Complaint alleged issues with the efficacy of masks marketed for COVID-19 protection. This is outside of OIG jurisdiction and was referred to the appropriate federal agency.

20-47 Complaint alleged issues with consistently malfunctioning evaporation coils on condenser units. This is outside of OIG jurisdiction and was referred to agency management.

20-48 Complainant was calling for information on a recalled electrical panel. This is outside of OIG jurisdiction and complainant was referred to agency management.

20-49 Complaint alleged a phishing scam. This is outside of OIG jurisdiction and was referred to the appropriate state and federal agencies.

20-50 Complaint reported a defective refrigerator. This is outside of OIG jurisdiction and was referred to agency management.

20-51 Complainant alleged retaliation from a railroad company. This is outside of OIG jurisdiction and the complainant was referred to the appropriate state and federal agencies.

20-52 Complaint alleged a wrongful termination at a dental office. This is outside of OIG jurisdiction and was referred to an appropriate state agency.

20-53 Complaint alleged spoof emails sent to vendors supposedly from an agency employee. This is outside of OIG jurisdiction and was referred to the appropriate federal agency.

20-54 Complaint alleges ethical and legal issues related to agency contracts with social media influencers. The complaint is currently under investigation.

20-55 Complaint alleged sales of counterfeit face masks. This complaint is outside of OIG jurisdiction and was referred to the appropriate federal agency.

20-56 Complainant was looking for the proper point of contact to verify a baby product importation certificate. This is outside of OIG jurisdiction and complainant was referred to agency management.

20-57 Complainant was seeking information regarding a whistleblower complaint related to a Native American Tribe. This complaint is outside of OIG jurisdiction and complainant was referred to another federal OIG.

20-58 Complaint alleged issues with a member of agency management. This complaint is currently under investigation.

20-59 Complaint alleged local employer was not taking safety precautions related to COVID-19. This is outside of OIG jurisdiction and was referred to the appropriate state agency.

20-60 Complaint regarding undue influence over a last will and testament. This is outside of OIG jurisdiction and was referred to the appropriate state agencies.

20-61 Complaint alleging unsafe baby teething rings for sale on a social media site. This is outside OIG jurisdiction and was referred to agency management.

20-62 Complaint alleged a local EMS/Fire Department was not responding to calls related to COVID-19 cases. This is outside of OIG jurisdiction and was referred to the appropriate state agencies.

20-63 Complaint alleged the blocking of online sales of cribs that were not part of a recall. This is outside of OIG jurisdiction and was referred to agency management.

20-64 Complaint alleged washing machines were rusting at the bleach dispenser. This is outside of OIG jurisdiction and was referred to agency management.

20-65 Complaint alleged a recalled doll was not listed on the company's recall page. This is outside of OIG jurisdiction and was referred to agency management.

20-66 Complaint alleged an oven was not on a recall list but has the same problem as other recalled ovens. This is outside of OIG jurisdiction and was referred to agency management.

20-67 Complaint alleged issues with mail delivery and its impact on mail-in voting. This is outside of OIG jurisdiction and was referred to the appropriate federal OIG.

20-68 Complaint regarding an ecommerce site that was shut down by the hosting platform. This is outside of OIG jurisdiction and was referred to the appropriate federal agency.

20-69 Complaint alleged a wrongful termination related to COVID-19. This is outside of OIG jurisdiction and was referred to the appropriate state agency.

20-70 Complaint alleged job retaliation at another federal agency. This is outside of OIG jurisdiction and was referred to the appropriate federal OIG.

20-71 Complaint alleged unsafe conditions at a public housing unit. This is outside of OIG jurisdiction and was referred to the appropriate state and federal agencies.

20-72 Complaint alleged unsafe windshields. This is outside of OIG jurisdiction and was referred to the appropriate federal agency.

20-73 Complaint alleged retaliation in the military for making a sexual harassment complaint. This is outside of OIG jurisdiction and was referred to the appropriate federal agency.

20-74 Complaint alleged retaliation from employer after refusing to remove asbestos in unsafe conditions. This is outside of OIG jurisdiction and was referred to the appropriate state and federal agencies.

20-75 Complaint alleged retaliation at a federal agency. This is outside of OIG jurisdiction and was referred to the appropriate federal agencies.

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
Consumer Product Safety Act
Consumer Product Safety Commission Regulations
Consumer Product Safety Improvement Act of 2008
Ethics Regulations
Executive Order on Combating Race and Sexual Stereotyping
Federal Acquisition Regulations
Federal Financial Management Improvement Act
Federal Information Security Modernization Act
Federal Sector Equal Employment Opportunity Complaint Processing Regulations
Freedom of Information Act
Hatch Act
Improper Payments Elimination and Recovery Improvement Act
Inspector General Act of 1978, as amended
Office of Management and Budget Circulars and Memoranda
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
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 Committee 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.

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.

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.	17
Section 5(a)(1)	Significant problems, abuses, and deficiencies.	3-5
Section 5(a)(2)	Recommendations with respect to significant problems, abuses, and deficiencies.	3-5
Section 5(a)(3)	Prior significant recommendations on which corrective action has not been completed.	6-10, 23-33
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.	3
Section 5(a)(7)	Summary of each particularly significant report.	3-5
Section 5(a)(8)	Table showing the number of audit, inspection, and evaluation reports and dollar value of questioned costs for reports.	22
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.	22
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.	6-10, 23-33
Section 5(a)(11)	Significant revised management decisions.	NA
Section 5(a)(12)	Significant management decisions with which the IG disagrees.	NA
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.	20
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.	20
Section 5(a)(17)	Statistical table showing total number of investigative reports, referrals, and results of referrals.	11
Section 5(a)(18)	Metrics used to develop data for table in section 5(a) (17).	11
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.	NA
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

OIG completes 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.

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 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 (USITC) Office of Inspector General. We gave USITC 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 Followup. 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 Blue Book 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
CLA	CliftonLarsonAllen, LLP
CPSC and Commission	U.S. Consumer Product Safety Commission
CPSRMS	Consumer Product Safety Risk Management System
DATA Act	Digital Accountability and Transparency Act
DPS	Defense Point Security
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information 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
IPERA	Improper Payments Elimination and Recovery Act
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
PSGP	Pool Safely Grants Program
QSIE	Quality Standards for Inspection and Evaluation
Treasury	Department of the Treasury
USITC	United States International Trade Commission
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 perid	0	$0.00	$0.00
Issued during period	1	$1,722,084.00	$0.00
Needing management decision during period	1	$1,722,084.00	$0.00
Management Decision Made During Period			
Amounts agreed to by management	1	$1,722,084.00	$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 reporting period, management continued to make progress in closing open recommendations. This chart provides a summary of reports issued before this reporting period with open recommendations as of the end the semiannual period, and shows progress made during the last six months.

Summary of Recommendation Implementation Progress						
Audit Short Title	Audit Date	Total Recom-mendations	Closed Prior to April 1, 2020	Open as of April 1, 2020	Closed during the period	Open as of September 30, 2020
RMS	6/5/2012	8	2	6	1	5
Debt	9/30/2014	2	0	2	0	2
FOIA	9/30/2015	11	4	7	0	7
Cybersecurity	8/14/2016	5	0	5	0	5
Contracts	7/25/2017	14	13	1	0	1
Telework	9/29/2017	9	4	5	0	5
OEP	6/7/2018	12	2	10	0	10
Directives	3/21/2019	2	1	1	0	1
Property	5/31/2019	25	2	23	1	22
Pentest	6/11/2019	40	16	24	8	16
		128	**44**	**84**	**10**	**74**

*This chart does not include any recommendations from the Financial Statement Audit and FISMA. Those recommendations, if any, are addressed in the annual audit process.

The table below shows all open recommendations from reports issued before this reporting period as of the end of the current semiannual period. As a reflection of the changing FISMA metrics, this table includes only the open recommendations from the most recent FISMA report prior to the current Semiannual Report period.

Report Name and Date	*Consolidated 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.
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.

Report Name and Date	*Consolidated Recommendations*
	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.
Report on the Performance Audit of Internal Controls over Contract Management and Administration for Fiscal Year 2016 (Contracts) July 25, 2017	Contracts-8. Obtain an attestation or audit of PRISM general and application controls routinely, preferably annually, and implement the resulting recommendations.
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.

Report Name and Date	*Consolidated Recommendations*
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.
	FISMA-1. Update the GSS system security plan compliance description for all NIST security controls and describe CPSC's process for developing and maintaining a comprehensive and accurate inventory of information systems. FISMA-2. Update the inventory of minor applications in the GSS system security plan to indicate which

Report Name and Date	*Consolidated Recommendations*
Evaluation of CPSC's FISMA Implementation for FY 2019 (FISMA) October 30, 2019	applications are in-house, third party, or cloud-hosted. FISMA-3. REDACTED FISMA-4. Develop, document, and implement a process for determining and defining system boundaries in accordance with NIST guidance. FISMA-5. Establish and implement a policy and procedures to manage software licenses using automated monitoring and expiration notifications. FISMA-6. REDACTED FISMA-7. 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 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). FISMA-8. REDACTED FISMA-9. REDACTED FISMA-10. REDACTED FISMA-11. REDACTED FISMA-12. REDACTED FISMA-13. Define and implement the identification and authentication policies and procedures. FISMA-14. REDACTED FISMA-15. Define and document a strategy (including specific milestones) to implement FICAM. FISMA-16. Integrate ICAM strategy and activities into the EA and ISCM. FISMA-17. 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.

Report Name and Date	*Consolidated Recommendations*
	FISMA-18. Perform an assessment of the knowledge, skills, and abilities of CPSC personnel with significant security responsibilities. FISMA-19. Develop and tailor security training content for all CPSC personnel with significant security responsibilities, and provide this training to the appropriate individuals. FISMA-20. Perform a gap analysis to identify all NIST SP 800-53 privacy controls from NIST SP 800-53, Appendix J that were not documented and assessed. FISMA-21. Document the implementation of all relevant privacy controls identified in the gap analysis in appropriate the system security plans. FISMA-22. Assess the implementation of all relevant privacy controls that were identified in the gap analysis. FISMA-23. Update the implementation statements for the PM family of controls in the GSS LAN's SSP to facilitate an assessment of the effectiveness of those controls. FISMA-24. Update the GSS LAN SSP to clearly indicate which controls are common controls and who is responsible for their implementation. FISMA-25. Develop an EA to be integrated into the risk management process. FISMA-26. Develop and implement a CM plan to ensure it includes all requisite information. FISMA-27. REDACTED FISMA-28. REDACTED FISMA-29. Further define the resource designations for a Change Control Board. FISMA-30. Identify and document the characteristics of items that are to be placed under CM control. FISMA-31. Establish measures to evaluate the implementation of changes in accordance with documented information system baselines and integrated secure configurations. FISMA-32. Define and document all the critical capabilities that the CPSC manages internally as part of the TIC program.

Report Name and Date	*Consolidated Recommendations*
	FISMA-33. Develop and document a robust and formal approach to contingency planning for agency systems and processes using the appropriate guidance (ex. NIST SP 800-34/53, FCD1, NIST CSF, and NARA guidance). FISMA-34. Develop, document, and distribute all required Contingency Planning documents (e.g. organization-wide COOP and BIA, Disaster Recovery Plan, BCPs, and ISCPs) in accordance with appropriate federal and best practice guidance. FISMA-35. Test the set of documented contingency plans. FISMA-36. Integrate documented contingency plans with the other relevant agency planning areas. FISMA-37. REDACTED FISMA-38. REDACTED FISMA-39. Establish and implement policies and procedures to require coordination between EXIT and FMPS to facilitate identification and incorporation of the appropriate clauses within all contracts. FISMA-40. Develop and implement an ERM program based on NIST 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 CPSC. FISMA-41. Identify, document, and implement a strategy to determine and define CPSC's risk appetite and tolerances, and apply this approach to prioritizing risk mitigation activities. FISMA-42. Develop and implement a supply chain risk management plan. FISMA-43. Integrate the established strategy for identifying organizational risk tolerance into the ISCM plan. FISMA-44. Establish and implement policies and procedures that require the documentation of POA&Ms with the OMB required level of granularity. FISMA-45. Establish appropriate dates to remediate issues reported and documented as part of the POA&M process.

Report Name and Date	*Consolidated Recommendations*
	FISMA-46. Track all changes to POA&M milestones and milestone dates. FISMA-47. Establish criteria to ensure analytics are performed on monthly reporting data and subsequently reported to management. FISMA-48. REDACTED FISMA-49. REDACTED FISMA-50. REDACTED FISMA-51. REDACTED FISMA-52. REDACTED FISMA-53. REDACTED FISMA-54. 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. FISMA-55. 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.

Report Name and Date	*Consolidated Recommendations*
Review of Personal Property Management System and Practices for the Calendar Year 2017 (PMS) May 31, 2019	PMS-1. Develop and implement a process for receiving and accepting goods and services in accordance with all applicable regulatory requirements. This process should include developing or adjusting an existing government form (e.g., receiving report) that meets these requirements to standardize the receipt and acceptance of goods and services at the CPSC. PMS-2. Provide training to CPSC personnel on the revised receipt and acceptance process. PMS-5. Develop and implement procedures to periodically inventory compliance sample items. 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-12. Establish and implement POA&M management procedures to ensure that estimated remediation timeframes are established for security weaknesses and based on the levels of risk and level of effort defined in the POA&Ms. 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

Report Name and Date	*Consolidated Recommendations*
	standard procedures for requesting and approving user access to roles and resources in PMS. 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-8. REDACTED PT-12. REDACTED PT-13. REDACTED PT-17. REDACTED

Report Name and Date	*Consolidated Recommendations*
	PT-18. REDACTED PT-20. REDACTED PT-29. REDACTED PT-32. REDACTED PT-33. REDACTED PT-35. REDACTED PT-36. REDACTED PT-38. REDACTED PT-39. REDACTED
AUDIT OF THE CPSC'S FINANCIAL STATEMENTS for FY 2019 November 19, 2019	FSA – 1. Establish a formal policy (i.e. desktop procedures) that defines the key roles and controls within the business process regarding leases. Management should update the policy periodically as necessary to reflect changes to the operation and communicate to all relevant parties for proper implementation. FSA – 2. Establish an appropriate communication and coordination protocol between the Office of Facilities Services, the Office of Financial Management, Planning and Evaluation and the third party service provider to ensure that all relevant documentation for lease activities is delivered timely and to the relevant personnel for proper tracking and accounting. FSA – 3. Enhance monitoring activities such as reconciliation between account balances recorded in the system and independent source documentation or reasonableness check comparing the invoice payments to lease/occupancy agreements. The results of these monitoring activities should have a separate evaluation to determine whether the controls are effective.

CONTACT US

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

Call:

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

On-line complaint form:

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

Write:

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