Office of Inspector General

U.S. Consumer Product Safety Commission

Semiannual Report to Congress

April 1, 2018 – September 30, 2018

October 30, 2018

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 OIG.

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; and

Work together to address Government-wide issues.

Office of Inspector General
U. S. Consumer Product Safety Commission

October 30, 2018

TO: Ann Marie Buerkle, Acting Chairman
Robert S. Adler, Commissioner
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, 2018, through September 30, 2018. The U.S. Consumer Product Safety Commission (CPSC) 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:

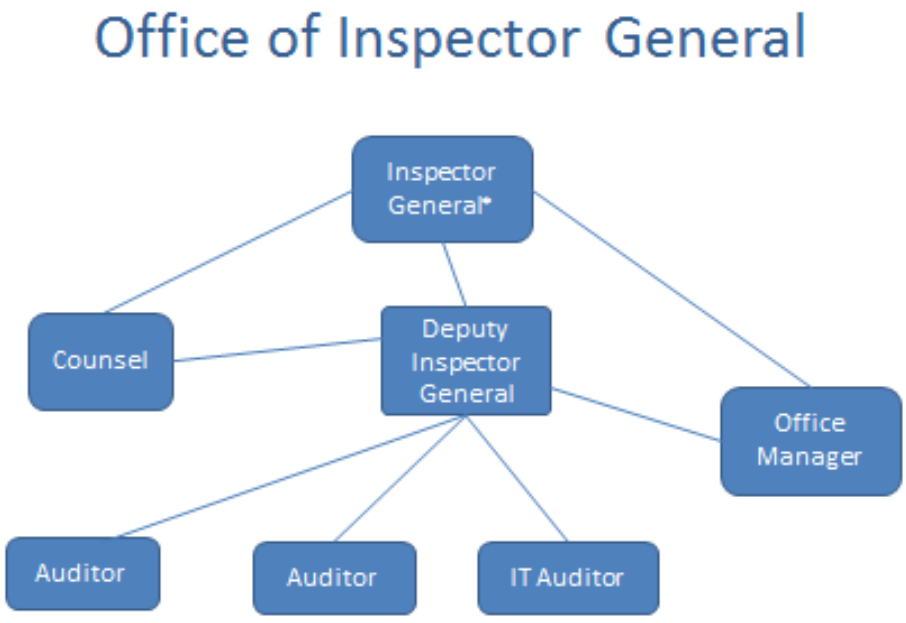
- conduct and supervise audits and investigations of the CPSC's programs and operations;

- 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; and

- keep the Commissioners and 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 sensible 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.



Audit Program

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

Completed Reports

REVIEW OF THE CPSC'S COMPLIANCE WITH THE IPERA FOR FY 2017
Transmitted: May 11, 2018
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 of 2010 (IPERA), as amended by the Improper Payments Elimination and Recovery Improvement Act of 2012, for transactions in Fiscal Year (FY) 2017. The review was performed in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Quality Standards for Inspections and Evaluations (QSIE). The review focused on the CPSC's compliance with the six elements identified as criteria in the Office of Management and Budget (OMB) Memorandum M-15-02 for payment accuracy, as well as overall program internal controls.

Kearney found that the CPSC was non-compliant with IPERA in FY 2017. This determination was based on three factors. First, the CPSC risk assessment process did not always attribute risk in a reasonable manner. Consequently, the CPSC was unnecessarily exposed to potential improper payments. Second, the CPSC did not obtain a statistically valid improper payment estimate for non-payroll activities consistent with the requirements of OMB M-15-02. Finally, the CPSC exceeded OMB's improper payment threshold of 10 percent by reporting an improper payment rate of 67 percent (about $21.1 of $31.3 million). It should be noted that the vast majority of these payments were improper because the individuals authorizing the payments lacked the legal authority to do so, not necessarily because the payments were fraudulent or wasteful. As a result of this report, Kearney made two recommendations to improve processes regarding controlling and reporting improper payments.

REVIEW OF VENDOR PAYMENTS FOR FY 2017
Transmitted: May 25, 2018
For the full report click here.

The OIG contracted with Kearney to perform a review of the CPSC's vendor payments. The FY 2016 IPERA compliance review identified a weakness in vendor payments processing. The objective of this review was to evaluate the CPSC's compliance with applicable financial management and contract laws and regulations for the approximately $27 million in vendor payments disbursed over the first three quarters of FY 2017. This review was performed in accordance with CIGIE QSIE. As a result of this review, Kearney found that the CPSC had not implemented sufficient internal controls over its vendor payment process to ensure that payments met all statutory and regulatory requirements prior to disbursement. Additionally, the CPSC had not recorded vendor payment adjustments in a timely manner. Kearney made 11 recommendations to improve the CPSC's management of vendor payments.

AUDIT OF THE OCCUPANT EMERGENCY PROGRAM FOR FISCAL YEAR 2017
Transmitted: June 7, 2018
For the full report click here.

The OIG audited the CPSC's Occupant Emergency Program in place for FY 2017. The purpose of an Occupant Emergency Program is to reduce the threat of harm to personnel, property, and other assets within the 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 generally accepted government auditing standards (GAGAS). Overall, we found that the CPSC's Occupant Emergency Program is not compliant with government-wide guidance and is not operating effectively. To improve the safety of CPSC employees we made 12 recommendations.

Ongoing Projects

AUDIT OF THE CONSUMER PRODUCT SAFETY COMMISSION'S FY 2018 FINANCIAL STATEMENTS

The OIG contracted with CliftonLarsonAllen, LLP, an independent public accounting firm, to perform an independent audit of the CPSC's financial statements according to all current standards, for the period ended September 30, 2018. 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.

IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT FOR FY 2018

The OIG contracted with Richard S. Carson & Associates, Inc. (Carson), a management consulting firm, to perform a review of the CPSC's compliance with the reporting requirements of the Federal Information Security Modernization Act (FISMA) for FY 2018. The objective of this review is to determine the effectiveness of the CPSC's information security program in accordance with the FY 2018 FISMA reporting requirements, issued by Department of Homeland Security and OMB Memorandum M-18-02. The review is being performed in accordance with CIGIE QSIE.

PENETRATION AND VULNERABILITY ASSESSMENT REPORT

The OIG contracted with Defense Point Security, a management consulting firm, to perform a penetration and vulnerability assessment of the CPSC network. The objective of this penetration test is to assess the security of the CPSC's information technology infrastructure by safely attempting to exploit security vulnerabilities. The review is being performed in accordance with CIGIE QSIE. The review focuses on the CSPC's resilience to cyberattack by outside actors.

PERSONAL PROPERTY MANAGEMENT REVIEW

The OIG contracted with Kearney to perform an assessment of the CPSC's control over personal property. The objective of this review is to obtain an independent review of the controls over personal property items, from initial data entry through routine accounting control to disposal. This review focuses on whether the CPSC's

internal control over personal property ensures efficient and effective use of CPSC resources in support of the Commission's mission. The review is being performed in accordance with CIGIE QSIE.

AUDIT OF THE CPSC'S DIRECTIVES SYSTEM

The OIG is conducting an audit on the CPSC's directives system. The objective of this audit is to determine whether the CPSC's policies and procedures for the directives system comply with federal regulations and procedures and are effective in helping the agency staff meet the CPSC's mission. This audit is being performed in accordance with GAGAS and focuses on the CPSC directives program prior to March 31, 2018.

CHARGE CARD RISK ASSESSMENT

The OIG initiated a risk assessment of the CPSC charge card programs. The objective of this review is to assess risks associated with the CPSC charge card programs for the purpose of planning future audits. The scope of our assessment will be limited to card activity and program management for the period April 1, 2017, to March 31, 2018, for the CPSC's purchase, travel, and fleet cards. The review is being performed in accordance with CIGIE QSIE.

Previously Issued Reports with Open Recommendations

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

CONSUMER PRODUCT SAFETY RISK MANAGEMENT SYSTEM INFORMATION SECURITY REVIEW REPORT
Transmitted: June 5, 2012
For the full report click here.

The objective of this review was to evaluate the application of the Risk Management Framework to the Consumer Product Safety Risk Management System (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 all eight 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.

FY 2013 THIRD-PARTY LABORATORY ACCREDITATION PROGRAM PERFORMANCE AUDIT
Transmitted: February 23, 2015
For the full report click here.

The objective of this audit was to assess the adequacy of the CPSC's procedures for accrediting laboratory assessment bodies. The OIG conducted this audit under GAGAS. This audit also included follow-up on the CPSC's implementation of recommendations from an earlier audit. We found that the CPSC had made significant improvements from the prior audit; however, the CPSC performed certain controls that were not documented in its written policies and procedures. 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 9 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 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 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 3 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 six remain open.

EVALUATION OF CPSC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014
Transmitted: October 31, 2017
For the full report click here.

The objective of this review was to determine the effectiveness of the CPSC's information security program in accordance with the FY 2017 FISMA reporting requirements issued by Department of Homeland Security and OMB. We contracted with Carson to perform this review in accordance with CIGIE QSIE. Carson found that the CPSC's information security program was not effective. However, Carson did note that the CPSC was making progress in implementing many of the FISMA requirements. Carson made 46 recommendations to improve the CPSC's information security posture. These recommendations will be reviewed as part of the FY 2018 FISMA review.

Investigative Program

The OIG investigates complaints and information received concerning possible violations of laws, rules, and regulations, as well as claims of mismanagement, abuse of authority, and waste of funds. These investigations are in response to allegations, complaints, and information received from CPSC's employees, other government agencies, contractors, and concerned individuals. The objective of this program is 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, 2018, to September 30, 2018.

Investigation Status	Count
Open as of April 1, 2018	5
Opened during reporting period	11
Closed during reporting period	6
Transferred to other Departments/Agencies	6
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, 2018	4

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

Reportable Investigations

18-12 Complaint alleged poor treatment during incarceration. The complaint was outside the jurisdiction of the OIG and complainant was referred to outside agencies for resolution.

18-13 Complaint alleged possible conflict of interest issues regarding a senior agency employee who was previously investigated for similar allegations (Complaint 18-05). A preliminary inquiry found no evidence of conflict of interest violations. The complaint was closed and not disclosed to the public.

18-14 Complaint alleged issues with a spirit board being used as part of a public school lesson for middle school students. Complainant already filed a report on Saferproducts.gov which was being processed by the agency. This complaint was outside of the jurisdiction of the OIG and is being resolved by the agency.

18-15 Complaint alleged issues with an employee working outside of normal business hours without permission. The complaint is currently under investigation.

18-16 Complaint alleged a senior official had violated 18 U.S.C. 205. A preliminary inquiry found that although the conduct alleged by the complainant had occurred, that conduct did not constitute a violation of 18 U.S.C. 205. The complaint was closed and not disclosed to the public.

18-17 Complaint alleged issues with a dental implant. This complaint was outside of the jurisdiction of the OIG and complainant was referred to an outside agency for resolution.

18-18 Complaint alleged issues with a reasonable accommodation. This complaint is currently under investigation.

18-19 Complaint alleged a company's products were being held up in customs due to possible violations. This complaint was outside of the jurisdiction of the OIG and referred to agency management for resolution.

18-20 Complaint alleged issues with postage paid to ship items internationally. The complaint was outside of the jurisdiction of the OIG and complainant was referred to an outside agency for resolution.

18-21 Complaint alleged issues with improper medical procedures involving a medical device. The complaint is closed due to lack of information from complainant.

18-22 Complaint alleged issues with possible improprieties by agency staff. The OIG requested more specific information but to date complainant has not responded. The complaint is closed.

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 Leave Act
Anti-Deficiency Act
Conflict of Interest Statute, 18 U.S.C. 205
Consumer Product Safety Act
Consumer Product Safety Improvement Act
Digital Accountability and Transparency Act
Dr. Chris Kirkpatrick Whistleblower Protection Act of 2017
Ethics Regulations
Federal Acquisition Regulations
Federal Information Security Modernization Act
Federal Travel Regulations
Fraud Reduction and Data Analytics Act of 2015
Freedom of Information Act
Government Charge Card Abuse Prevention Act
Hatch Act
Improper Payments Elimination and Recovery Improvement Act
Inspector General Act, as amended
Inspector General Empowerment Act of 2016
Inspector General Subpoena Authority Act, H.R. 4917
NARA General Records Schedules and Regulations
NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017
OMB Circulars
OPM Regulations on Administrative Leave Act
Privacy Program
Prohibited Personnel Practices
Records Management Policies and Regulations
Standards of Conduct for Government Employees
Telework Enhancement Act of 2010
Telework Policies
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 activities. CIGIE identifies, reviews, and discusses issues that are of interest to the entire OIG community. The IG 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.	14
Section 5(a)(1)	Significant problems, abuses, and deficiencies.	5-6
Section 5(a)(2)	Recommendations with respect to significant problems, abuses, and deficiencies.	5-6
Section 5(a)(3)	Prior significant recommendations on which corrective action has not been completed.	9-11, 19-25
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, evaluation reports by subject matter, showing dollar value of questioned costs and of recommendations that funds be put to better use.	NA
Section 5(a)(7)	Summary of each particularly significant report.	5-6
Section 5(a)(8)	Table showing number of audit, inspection, and evaluation reports and dollar value of questioned costs for reports.	NA
Section 5(a)(9)	Table showing 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.	9-11
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)	Info under section 804(b) of Federal Financial Management Improvement Act of 1996.	NA
Section 5(a)(14)	Results of peer review.	17
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.	17
Section 5(a)(17)	Statistical Tables showing total number of investigative reports, referrals, and results of referrals.	12
Section 5(a)(18)	Metrics used to develop data for tables in section 5(a) (17).	12
Section 5(a)(19)	Report on each investigation involving a senior government official where allegations of misconduct are substantiated.	NA
Section 5(a)(20)	Detailed description of whistleblower retaliation.	NA
Section 5(a)(21)	Detailed description of attempt to interfere with OIG independence.	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.	13

Appendix B: Peer Review

Generally accepted government auditing standards require each audit organization to obtain an external review of its system of quality control every three years and make the results publicly available.

On March 30, 2017, the National Endowment for the Humanities 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, 2016, had been "suitably designed and complied with to provide our office 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 with no accompanying letter of comment. A copy of this peer review is on our website.
For the full report click here.

The CPSC OIG last conducted a peer review in March 2016, for the National Credit Union Administration Office of Inspector General. No deficiencies were noted and no formal recommendations were made in that review. A letter of comment was issued to the National Credit Union Administration Office of Inspector General.

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	
Carson	Richard S. Carson & Associates, Inc.
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CPSC	U.S. Consumer Product Safety Commission
CPSRMS	Consumer Product Safety Risk Management System
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
IG Act	The Inspector General Act of 1978, as amended
IPERA	Improper Payments Elimination and Recovery Act
Kearney	Kearney & Company
OIG	Office of Inspector General
OMB	Office of Management and Budget
QSIE	Quality Standards for Inspection and Evaluation

Appendix D: Consolidated List of Open Recommendations

During this reporting period, management continued to make progress in closing open recommendations. In addition, as a reflection of the changing FISMA metrics, this table includes only the recommendations from the most recent FISMA report.

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-5. Update the POAM to include the missing information, as required by OMB M-4-25. RMS-6. Perform an assessment to ensure the adequate categorization of information types. RMS-7. Analyze and document whether all of the information types outlined in the NIST 800-60 framework were appropriately included or excluded from the CPSRMS Security Categorization 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.
FY 2013 Third-Party Laboratory Accreditation Program Performance Audit (Lab) February 23, 2015	Lab-1. Establish policies and procedures to document: 1) the actions performed by the CPSC when there is a delay in a laboratory's submission of a valid CPSC Audit or Update Certificate application, and 2) criteria for deregistration. Lab-2. Establish policies and procedures to document its due diligence over ensuring that Independent Laboratory Accreditation Cooperation is carrying out its testing and accreditation of laboratories to support certification by CPSC.

Report Name and Date	*Consolidated Recommendations*
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–4. Management log all FOIA requests received into the FOIAXpress system or similar non-electronic system where information is retrievable. FOIA–5. Management develops a record retention schedule that complies with all current document retention requirements. FOIA–6. Management develop 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–9. Management should review and publish an updated fee schedule regularly, at least annually. 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.

Report Name and Date	*Consolidated Recommendations*
Report on the Performance Audit of Internal Controls over Contract Management and Administration for Fiscal Year 2016 (Contracts) July 25, 2017	Contracts-3. Create and implement policies and procedures for COs to periodically monitor COR contract administration files. Procedures should include requirements for documenting the monitoring and any resulting recommendations. This monitoring document should be maintained as part of the contract administration file. Contracts-8. Obtain an attestation or audit of PRISM general and application controls routinely, preferably annually, and implement the resulting recommendations. Contracts-12. Develop policies and procedures for evaluating and monitoring the quality of data. Procedures should use data to identify and evaluate high-risk indicators and realize efficiencies in the contract management process.
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. Telework-6. Train all telework participants, supervisors, and other staff who review and use this data, on how to use telework indicators in the timekeeping system.
Evaluation of CPSC's Implementation of the Federal Information Security Modernization Act of 2014 (FISMA 2014) October 31, 2017	FISMA-1. 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-2. Develop, document, and distribute all required Contingency Planning documents (ex. organization-wide COOP and BIA, Disaster Recovery Plan, BCPs, and ISCPs) in accordance with appropriate federal and best practice guidance. FISMA-3. Test the set of documented contingency plans. FISMA-4. Integrate documented contingency plans with the other relevant agency planning areas.

Report Name and Date	*Consolidated Recommendations*
	FISMA-5. Develop and enforce a CM plan to ensure it includes all requisite information. FISMA-6. REDACTED FISMA-7. Identify and document the characteristics of items that are to be placed under CM control. FISMA-8. Establish measures to evaluate, coordinate, and approve/disapprove the implementation of configuration changes. FISMA-9. REDACTED FISMA-10. Further define the resource designations for a Configuration Control Board. FISMA-11. Define and document all the critical capabilities that the CPSC manages internally as part of the TIC program Managed Trusted Internet Protocol Service. FISMA-12. Fully implement the CM policies and procedures. FISMA-13. REDACTED FISMA-14. REDACTED FISMA-15. Develop an Enterprise Architecture to be integrated into the Risk Management Process. FISMA-16. Utilize the existing implementation of the Network Inventory and Integrated Asset Management solution to track and manage software licenses. FISMA-17. REDACTED FISMA-18. Define and document the taxonomy of the CPSC's systems to be classified as one of the following types: IT system (e.g., proprietary and/or owned by the CPSC), application (e.g., commercial off-the-shelf, government off-the-shelf, or custom software), laptops and/or personal computers, service (e.g., external services that support the CPSC's operational mission, facility, or Social Media). FISMA-19. Develop, document, and implement a process that identifies the CPSC's approach around determining and defining system boundaries. FISMA-20. Develop, document, and implement a process to classify agency systems as "major" or "minor" in accordance with OMB Circular A-130. FISMA-21. REDACTED FISMA-22. REDACTED

Report Name and Date	*Consolidated Recommendations*
	FISMA-23. Establish a policy and strategy to identify the CPSC's approach to manage software licenses around automated monitoring and expiry notifications. FISMA-24. REDACTED FISMA-25. REDACTED FISMA-26. Implement the identification and authentication policies and procedures. FISMA-27. Automatically revoke temporary and emergency access after a specified period of time. FISMA-28. Develop and implement an ERM program based on guidance from the ERM Playbook (A-123, Section II requirement). FISMA-29. Identify, document, and implement a strategy to determine the organizational risk tolerance and adequately document the approach in the Risk Management Strategy, policies, and procedures. FISMA-30. Integrate the established strategy for identifying organizational risk tolerance into the ISCM plan. FISMA-31. Establish and implement policies and procedures to require coordination between EXIT and procurement to facilitate identification and incorporation of the appropriate contract clauses within all contracts. FISMA-32. Define and document a strategy (that includes specific milestones) to implement FICAM. FISMA-33. Integrate the FICAM Strategy and activities into the Enterprise Architecture and ISCM. FISMA-34. Perform an assessment of the knowledge, skills, and abilities of all CPSC personnel with significant security responsibilities. FISMA-35. Modify the Security and Awareness Training policy to ensure CPSC personnel that affect security (e.g., Executive Risk Council and the roles outlined in 5 CFR 930.301) are required to participate in role-based and/or specialized training. FISMA-36. Develop/tailor security training content for all CPSC personnel with significant security responsibilities. FISMA-37. Develop/tailor security awareness training and role-based security training content that reflects the agency's organization, requirements, types of systems, culture, mission, and risk environment. FISMA-38. Provide role-based security training to all CPSC users who affect security.

Report Name and Date	*Consolidated Recommendations*
	FISMA-39. Develop and distribute an organization-wide information security program plan. FISMA-40. Implement and assess the effectiveness of the PM controls, as documented in the information security program plan. FISMA-41. Establish and implement policies and procedures that require the documentation of POAMs with the OMB required level of granularity. FISMA-42. Establish appropriate dates to remediate issues reported and documented as part of the POAM process. FISMA-43. Establish criteria to ensure analytics are performed on monthly reporting data and subsequently reported to management. FISMA-44. Perform a gap analysis to identify all NIST SP 800-53, rev 4 security controls that were not documented and assessed. FISMA-45. Document the implementation of all relevant security controls identified in the gap analysis. FISMA-46. Assess the implementation of all relevant security controls that were identified in the gap analysis.
Review of the CPSC's Compliance with IPERA for FY 2017 May 11, 2018	IPERA 17-1. Develop and implement an effective IPERA risk assessment that provides adequate consideration to non-payroll activities. IPERA 17-2. Implement policies and procedures for performing and reporting improper payments that are consistent with OMB M-15-02 (e.g., performing qualitative and quantitative risk assessments and obtaining a statistically valid estimate of improper payments for activities susceptible to significant improper payments).
Review of Vendor Payments in FY 2017 (Vendor) May 25, 2018	Vendor-1. Create and implement policies and procedures for FMFS personnel to annually review the ESC SSAE-18 report, identify complementary user entity controls as recommended by ESC, and implement those controls. Vendor-2. Develop a checklist to assist invoice approvers in ensuring the completeness and accuracy of vendor packages prior to payment disbursement. This checklist should include all of the CPSC required elements for a proper payment. Vendor-3. Provide training to EXFM personnel on requirements for proper payments. Vendor-4. 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., DD 250) that meets these requirements to standardize the receipt and acceptance of goods and services at the CPSC. Vendor-5. Provide training to CPSC personnel on the revised receipt and acceptance process.

Report Name and Date	*Consolidated Recommendations*
	Vendor-6. Develop and implement policies and procedures for monitoring and remediating the quality of data. These procedures should include the use of data to realize efficiencies in the contract management process and ensure the timely deobligation of undelivered orders. Vendor-7. Provide training to EXFM personnel related to evaluating the accuracy of the data.
Audit of the Occupant Emergency Program for Fiscal Year 2017 June 7, 2018	OEP-1. Clearly define all the roles to be used in the agency's OEP. OEP-2. Develop and implement a process to keep OEP team member and occupant lists up-to-date. 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. OEP-12. Develop and implement effective coordination with other federal tenants in Bethesda Towers.

CONTACT US

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

Call: Inspector General's HOTLINE: 301-504-7906
Or: 1-866-230-6229

On-line complaint form:

Click here for complaint form.

Click here for CPSC OIG Website.

Or **Write:**

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