



Office of Inspector General

U.S. Consumer Product Safety Commission

Semiannual Report to Congress
October 1, 2018 – March 31, 2019

April 30, 2019

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; and

Work together to address government-wide issues.



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

April 30, 2019

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 October 1, 2018, through March 31, 2019. 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	3
U.S. Consumer Product Safety Commission	3
Office of Inspector General	3
Audit Program	5
Completed Reports	5
Ongoing Projects	7
Previously Issued Reports with Open Recommendations	9
Investigative Program	13
Reportable Investigations	13
Other Activities	15
Legislation and Regulatory Review	15
OIG Coordination	16
Appendix A: Cross-Reference to Reporting Requirements of the IG Act	17
Appendix B: Peer Review	18
Appendix C: Statement Regarding Plain Writing	19
Appendix D: Consolidated List of Open Recommendations.....	20

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.

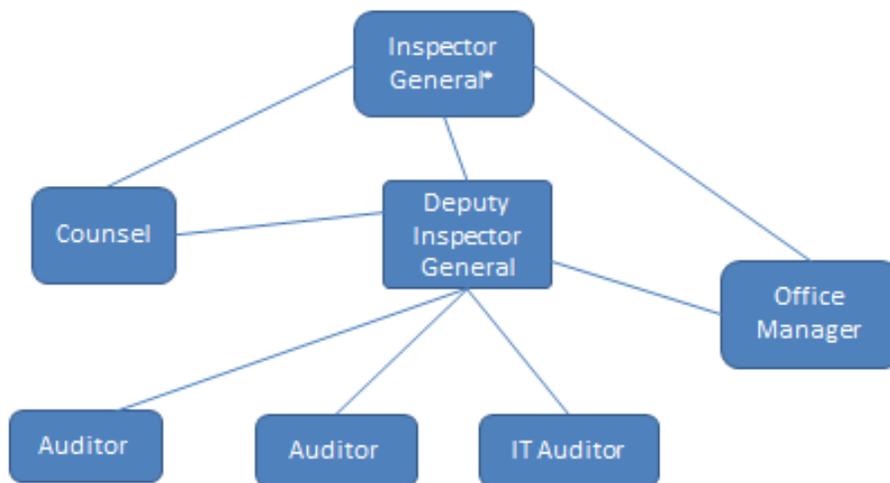
The IG Act was amended by the Inspector General Empowerment Act of 2016. The Inspector General Empowerment Act safeguards OIG access to agency information and mandates additional reporting to increase transparency in government operations.

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 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 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.

Office of Inspector General



Audit Program

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

Completed Reports

EVALUATION OF CPSC'S FISMA IMPLEMENTATION FOR FY 2018

Transmitted: October 31, 2018

For the full report [click here](#)

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 Fiscal Year (FY) 2018. The objective of this review was to determine the effectiveness of the CPSC's information security program in accordance with the FY 2018 FISMA reporting requirements, issued by the Department of Homeland Security and Office of Management and Budget (OMB) Memorandum M-18-02. The review was performed in accordance with Council of Inspectors General for Integrity and Efficiency (CIGIE) Quality Standards for Inspection and Evaluation (QSIE).

Carson found that the CPSC was not compliant with all of FISMA's requirements. However, the CPSC was making progress in implementing many of FISMA requirements. Carson made 52 recommendations to improve the CPSC's information security posture.

AUDIT OF THE CPSC'S FINANCIAL STATEMENTS FOR FY 2018

Transmitted: November 7, 2018

For the full report [click here](#)

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 was 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 was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS).

In CliftonLarsonAllen'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, 2018, and 2017, in conformity with accounting principles generally accepted in the United States of America.

RISK ASSESSMENT OF THE CPSC'S CHARGE CARD PROGRAMS

Transmitted: December 21, 2018

For the full report [click here](#)

The OIG initiated a risk assessment of the CPSC charge card programs. The objective of this review was to assess risks associated with the CPSC charge card programs for the purpose of planning future audits. The scope of our risk assessment was 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 was performed in accordance with CIGIE QSIE.

Overall, we concluded that the risk of illegal, improper, or erroneous purchases and payments through the CPSC's charge card programs during the scope period was low for the purchase and fleet card programs and medium for the travel card program.

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. These recommendations will provide more current information and improve stakeholder access.

Ongoing Projects

AUDIT OF THE CPSC'S POOL SAFELY GRANTS PROGRAM

The OIG is auditing the CPSC's Pool Safely Grants Program (PSGP) for all grants awarded prior to September 30, 2018. The PSGP provides awardees assistance to implement enforcement and education programs to prevent the drowning and drain entrapments of children in pools and spas. The objective of this audit is to assess agency compliance with the laws and regulations that govern the PSGP, the overall effectiveness of the PSGP, and the adequacy of the agency's internal controls over the program. The audit is being performed in accordance with GAGAS.

AUDIT OF THE CPSC'S FY 2019 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, 2019. 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.

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 CPSC's resilience to cyberattack by outside actors.

PERSONAL PROPERTY MANAGEMENT REVIEW

The OIG contracted with Kearney & Company (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.

REVIEW OF THE CPSC'S COMPLIANCE WITH THE IPERA FOR FY 2018

The OIG contracted with 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 (IPERIA), for transactions in FY 2018. The review is being performed in accordance with CIGIE QSIE. The review focuses on the CPSC's compliance with the six elements identified as criteria in OMB's M-18-20 for payment accuracy, as well as overall program internal controls.

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 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 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 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.

REVIEW OF THE CPSC'S COMPLIANCE WITH THE IPERA FOR FY 2017

Transmitted: May 11, 2018

For the full report [click here](#).

The objective of this review was to assess the CPSC's compliance with the requirements contained in IPERA, as amended by IPERIA, for FY 2017. The OIG contracted with Kearney to perform this review in accordance with CIGIE QSIE. The review focused on the CPSC's compliance with the six elements identified as criteria for payment accuracy in OMB's Memorandum M-15-02 as well as on overall program internal controls. The report made two recommendations to improve the program and both remain open.

AUDIT OF THE OCCUPANT EMERGENCY PROGRAM FOR FISCAL YEAR 2017

Transmitted: June 7, 2018

For the full report [click here](#).

The OIG audited the CPSC's Occupant Emergency Program in place for FY 2017. The purpose of an Occupant Emergency Program is to reduce the threat of harm to personnel, property, and other assets within a federal facility in the event of an emergency. The 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 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 and all remain open.

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 October 1, 2018, to March 31, 2019.

Investigation Status	Count
Open as of October 1, 2018	4
Opened during reporting period	10
Closed during reporting period	3
Transferred to other Departments/Agencies	5
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 March 31, 2019	6

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

Reportable Investigations

19-01 Anonymous complaint alleged improprieties regarding pesticide label. The complaint was closed because the complaint is outside the jurisdiction of the OIG and there was no contact information to facilitate a referral to another agency.

19-02 Complaint alleged property was contaminated with sewage. This complaint is outside of the jurisdiction of the OIG and was referred to outside agencies for resolution.

19-03 Complaint alleged a lack of response to a previous consumer complaint. This complaint was transferred to the agency and the OIG is monitoring the agency response.

19-04 Complaint alleged issues with agency oversight of data collection. The complaint is currently under investigation.

19-05 Complaint alleged whistleblower retaliation on local and county level due to disclosures made regarding janitorial cleaning practices at a public school. This complaint is outside of the jurisdiction of the OIG and was referred to outside agencies for resolution.

19-06 Complaint alleged issues with a tankless water heater. This complaint is currently under investigation.

19-07 Complaint alleged issues with a thrift store reselling jewelry online. This investigation was closed due to lack of information from complainant.

19-08 Complaint alleged a furniture company's poor storage methods led to a bedbug infestation. This complaint is outside of the jurisdiction of the OIG and complainant was referred to outside agencies for resolution.

19-09 Complaint alleged issues with a package delivery. The complaint is outside of the jurisdiction of the OIG and complainant was referred to an outside agency for resolution.

19-10 Complaint alleged whistleblower retaliation under American Recovery and Reinvestment Act of 2009. This complaint is outside of the jurisdiction of the OIG and complainant was referred to the appropriate agency for resolution.

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 Improvement Act
Digital Accountability and Transparency Act
Dr. Chris Kirkpatrick Whistleblower Protection Act of 2017
Ethics Regulations
Federal Acquisition Regulations
Federal Employee Antidiscrimination Act of 2019, H.R. 135
Federal Information Security Modernization Act
Federal Sector Equal Employment Opportunity Complaint Processing Regulations
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
National Archives and Records Administration General Records Schedules and Regulations
National Institute of Standards and Technology Cybersecurity Framework, Assessment, and Auditing Act of 2017
OMB Circulars
Office of Personnel Management Regulations on Administrative Leave Act
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 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.	15
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.	9-12, 20-26
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.	9-12
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.	18
Section 5(a)(15)	Outstanding recommendations from any peer review conducted by another OIG.	NA
Section 5(a)(16)	Any peer reviews performed of another OIG.	18
Section 5(a)(17)	Statistical table showing total number of investigative reports, referrals, and results of referrals.	13
Section 5(a)(18)	Metrics used to develop data for table in section 5(a) (17).	13
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 Review

GAGAS 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 completed a peer review on March 20, 2019, for the United States International Trade Commission Office of Inspector General. We gave an External Peer Review rating of pass with no accompanying letter of comment. No deficiencies were noted and no formal recommendations were made in that review.

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 Modernization 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
IPERIA	Improper Payments Elimination and Recovery Improvement Act
Kearney	Kearney & Company
OIG	Office of Inspector General
OMB	Office of Management and Budget
PSGP	Pool Safety Grants Program
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.

<i>Report Name and Date</i>	<i>Consolidated Recommendations</i>
<p>Consumer Product Safety Risk Management System Information Security Review Report (RMS)</p> <p>June 5, 2012</p>	<p>RMS-1. Identify the participants of the CPSC Risk Executive Council and define specific tasks/milestones for implementing the proposed Risk Management Framework.</p> <p>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.</p> <p>RMS-3. Fully document the implementation of the security controls.</p> <p>RMS-4. Update the CPSRMS SSP to be the single authoritative system security document.</p> <p>RMS-5. Update the POAM to include the missing information, as required by OMB M-4-25.</p> <p>RMS-6. Perform an assessment to ensure the adequate categorization of information types.</p> <p>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.</p> <p>RMS-8. Define the specific Public Access controls in place/planned.</p>
<p>Opportunities Exist to Ensure CPSC Employees Are Satisfying in Good Faith Their Just Financial Obligations (Debt)</p> <p>September 30, 2014</p>	<p>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.</p> <p>DEBT-2. Management develops a process to regularly, at least annually, review employee exemption and withholding status for reasonableness.</p>
<p>FY 2013 Third-Party Laboratory Accreditation Program Performance Audit (Lab)</p> <p>February 23, 2015</p>	<p>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.</p> <p>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.</p>

<i>Report Name and Date</i>	<i>Consolidated Recommendations</i>
<p>Audit of the Freedom of Information Act Program (FOIA)</p> <p>September 30, 2015</p>	<p>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.</p> <p>FOIA-3. Management develops SOP consistent with current FOIA legislation related to receipt, processing, and tracking of FOIA requests for IDI files.</p> <p>FOIA-5. Management develops a record retention schedule that complies with all current document retention requirements.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>FOIA-11. Management documents a review of the data fields in [REDACTED] for accuracy, completeness, and timeliness.</p>
<p>Cybersecurity Information Sharing Act of 2015 Review Report (Cyber)</p> <p>August 14, 2016</p>	<p>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.</p> <p>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.</p> <p>Cyber-3. The General Access Control Policy and attendant procedures should be updated to include the elements outlined in the report.</p> <p>Cyber-4. Develop, document, and maintain a software inventory including license management policies and procedures.</p> <p>Cyber-5. Comply with and enforce HSPD-12 multifactor authentication supported by the Personal Identity Verification Card.</p>
<p>Report on the Performance Audit of Internal Controls over Contract Management and Administration for Fiscal Year 2016 (Contracts)</p> <p>July 25, 2017</p>	<p>Contracts-8. Obtain an attestation or audit of [REDACTED] general and application controls routinely, preferably annually, and implement the resulting recommendations.</p>

<i>Report Name and Date</i>	<i>Consolidated Recommendations</i>
<p>Audit of the Telework Program for Fiscal Year 2016 (Telework)</p> <p>September 29, 2017</p>	<p>Telework-1. Develop and implement a telework policy that is compliant with current federal laws, regulations, and OPM best practices where appropriate.</p> <p>Telework-2. Align agency practice and telework policy regarding employee participation and position eligibility.</p> <p>Telework-3. Document all decisions made with regard to position eligibility, individual participation including policy exceptions, participation limits, and termination of telework agreements.</p> <p>Telework-4. Design and implement a process to ensure that telework files are complete and regularly reviewed, at least biennially.</p> <p>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.</p>
<p>Review of the CPSC's Compliance with IPERA for FY 2017</p> <p>May 11, 2018</p>	<p>IPERA 17-1. Develop and implement an effective IPERA risk assessment that provides adequate consideration to non-payroll activities.</p> <p>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)</p>
<p>Audit of the Occupant Emergency Program for Fiscal Year 2017</p> <p>June 7, 2018</p>	<p>OEP-1. Clearly define all the roles to be used in the agency's OEP.</p> <p>OEP-2. Develop and implement a process to keep OEP team member and occupant lists up-to-date.</p> <p>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.</p> <p>OEP-4. Develop and implement policies employing multiple communication channels for notifying staff during drills and emergency situations.</p> <p>OEP-5. Develop and implement occupant accountability procedures to be practiced during drills and used during emergencies.</p> <p>OEP-6. Develop and implement an effective OEP team training program with drills and exercises to include all team members at least annually.</p> <p>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.</p> <p>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.</p>

<i>Report Name and Date</i>	<i>Consolidated Recommendations</i>
	<p>OEP-9. Develop and implement procedures to maintain, retain, and update OEP program documents at least semiannually.</p> <p>OEP-10. Develop and implement an annual round-table discussion with OEP coordinators and teams.</p> <p>OEP-11. Develop and implement facility-specific policies and procedures.</p> <p>OEP-12. Develop and implement effective coordination with other federal tenants in Bethesda Towers.</p>
<p>Evaluation of CPSC's Implementation of the Federal Information Security Modernization Act of 2014 (FISMA 2014)</p> <p>October 31, 2018</p>	<p>FISMA-1. Obtain completed annual A&A packages with valid ATO for all of the CPSC's major systems.</p> <p>FISMA-2. REDACTED.</p> <p>FISMA-3. Develop, document, and implement a process for determining and defining system boundaries in accordance with NIST guidance.</p> <p>FISMA-4. Develop, document, and implement a process to classify agency systems as "major" or "minor" in accordance with OMB Circular A-130.</p> <p>FISMA-5. Establish and implement a policy and procedures to manage software licenses using automated monitoring and expiration notifications.</p> <p>FISMA-6. REDACTED</p> <p>FISMA-7. 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) in accordance with FEA.</p> <p>FISMA-8. REDACTED</p> <p>FISMA-9. REDACTED</p> <p>FISMA-10. REDACTED</p> <p>FISMA-11. Define and implement identification and authentication policies and procedures.</p> <p>FISMA-12. Automatically revoke temporary and emergency access after a specified period of time.</p> <p>FISMA-13. Define and document a strategy (which include specific milestones) to implement FICAM.</p> <p>FISMA-14. Integrate ICAM strategy and activities into the enterprise architecture and ISCM.</p> <p>FISMA-15. Modify the Security and Awareness Training policy to ensure CPSC personnel that affect security and privacy (e.g., Executive Risk Council) are required to participate in role- based and/or specialized training.</p>

<i>Report Name and Date</i>	<i>Consolidated Recommendations</i>
	<p>FISMA-16. Perform an assessment of the knowledge, skills, and abilities of CPSC personnel with significant security responsibilities.</p> <p>FISMA-17. Develop/tailor security training content for all CPSC personnel with significant security responsibilities, and provide this training to the appropriate individuals.</p> <p>FISMA-18. Perform a gap analysis to identify all NIST SP 800-53, Rev 4 security controls that were not documented and assessed.</p> <p>FISMA-19. Document the implementation of all relevant security controls identified in the gap analysis.</p> <p>FISMA-20. Assess the implementation of all relevant security controls that were identified in the gap analysis.</p> <p>FISMA-21. Update the implementation statements for the program management family of controls in the GSS LAN's SSP to facilitate an assessment of the effectiveness of those controls.</p> <p>FISMA-22. Update the GSS LAN SSP to clearly indicate which controls are common controls, and who is responsible for their implementation.</p> <p>FISMA-23. Update the CPSC ISCM Plan to specify the assessment frequency, monitoring frequency, and annual assessment testing schedule for the program management family of security controls, and the privacy controls.</p> <p>FISMA-24. Develop an EA to be integrated into the Risk Management Process.</p> <p>FISMA-25. Develop and enforce a CM plan to that ensures it includes all requisite information.</p> <p>FISMA-26. Develop and implement a set of CM procedures in accordance with the inherited CM Policy which includes appropriate measures for all hardware, software, and supporting infrastructure (e.g., equipment, networks, and operating systems).</p> <p>FISMA-27. REDACTED</p> <p>FISMA-28. Further define the resource designations for a Change Control Board.</p> <p>FISMA-29. Identify and document the characteristics of items that are to be placed under CM control.</p> <p>FISMA-30. Establish measures to evaluate, coordinate, and approve/disapprove the implementation of changes.</p> <p>FISMA-31. REDACTED</p>

<i>Report Name and Date</i>	<i>Consolidated Recommendations</i>
	<p>FISMA-32. Define and document all the critical capabilities that the CPSC manages internally as part of the TIC program Managed Trusted Internet Protocol Service.</p> <p>FISMA-33. Develop and document a robust and formal approach to contingency planning for agency systems and processes using the appropriate guidance (e.g., NIST SP 800-34/53, FCD1, NIST CSF, and NARA guidance).</p> <p>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.</p> <p>FISMA-35. Test the set of documented contingency plans.</p> <p>FISMA-36. Integrate documented contingency plans with the other relevant agency planning areas.</p> <p>FISMA-37. Develop, document, and distribute all required procedures for the destruction or reuse of media containing PII or other sensitive agency data (e.g., proprietary information).</p> <p>FISMA-38. REDACTED</p> <p>FISMA-39. REDACTED</p> <p>FISMA-40. 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.</p> <p>FISMA-41. Develop and implement an ERM program based on NIST guidance and guidance from the ERM Playbook (A-123, Section II requirement). This includes establishing a cross-departmental risk executive (function) lead by senior management to provide both a departmental and organization level view of risk to the top decision makers within the CPSC.</p> <p>FISMA-42. 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.</p> <p>FISMA-43. Integrate the established strategy for identifying organizational risk tolerance into the ISCM plan.</p> <p>FISMA-44. Establish and implement policies and procedures that require the documentation of POA&Ms with the OMB-required level of granularity.</p> <p>FISMA-45. Establish appropriate dates to remediate issues reported and documented as part of the POA&M process.</p> <p>FISMA-46. Track all changes to POA&M milestones and milestone dates.</p> <p>FISMA-47. Establish criteria to ensure analytics are performed on monthly reporting data and subsequently reported to management.</p>

<i>Report Name and Date</i>	<i>Consolidated Recommendations</i>
	<p>FISMA-48. REDACTED</p> <p>FISMA-49. REDACTED</p> <p>FISMA-50. REDACTED</p> <p>FISMA-51. Identify and implement appropriate profiling techniques to baseline network operations and the characteristics of expected data flows for users and systems.</p> <p>FISMA-52. REDACTED</p>
<p>Audit of the CPSC's Directives System</p> <p>March 21, 2019</p>	<p>Directives-1. Complete the online directives reading room currently under construction at CPSC.gov.</p> <p>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.</p>

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.



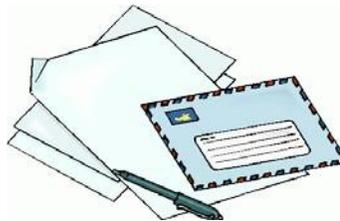
Call: Inspector General's HOTLINE: 301-504-7906
Or: 1-866-230-6229



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