Office of Inspector General

U.S. Consumer Product Safety Commission

Semiannual Report to Congress
October 1, 2017 – March 31, 2018

April 30, 2018

Vision Statement

We are agents of positive change striving for continuous improvements in our agency's management and program operations.

Statement of Principles

We will:

Work with the Commission and 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, 2018

TO: Ann Marie Buerkle, Acting Chairman
Robert S. Adler, Commissioner
Elliot F. Kaye, Commissioner
Marietta S. Robinson, 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, 2017, through March 31, 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 Commissioners, 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

The 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 (P.L. 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 (CPSIA). 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 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 (IG) in 2004.

The IG Act was recently amended by the Inspector General Empowerment Act of 2016, signed into law on December 16, 2016. The Inspector General Empowerment Act safeguards OIG access to agency information and mandates additional reporting to increase transparency in government operations.

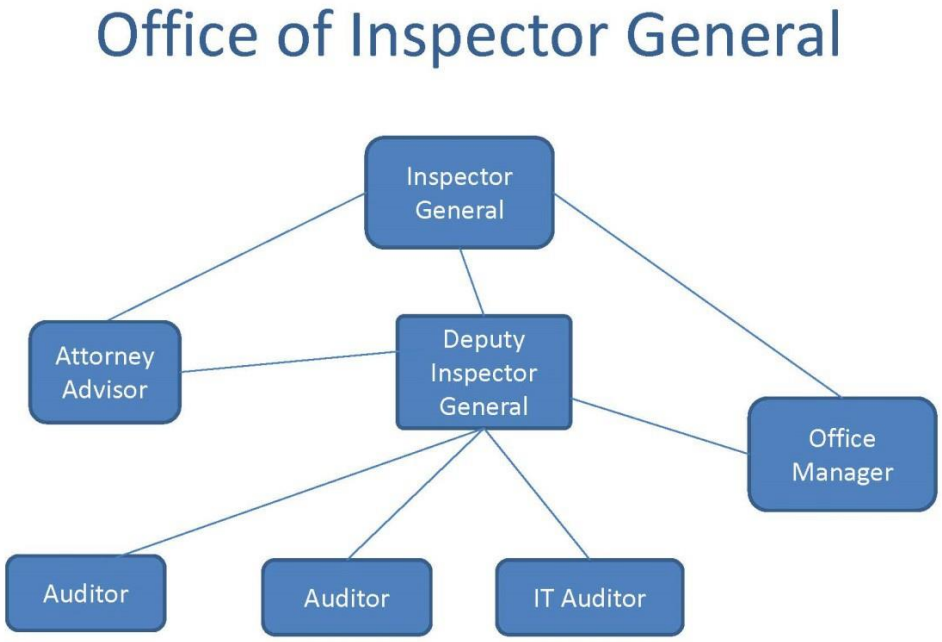
The IG Act gives the Inspector General the authority and responsibility to:

- 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 semi-annual period, the OIG completed three audits or reviews. At the end of the reporting period four audits or reviews remained ongoing.

Completed Reports

FEDERAL INFORMATION SECURITY MODERNIZATION ACT REVIEW REPORT FOR FY 2017
Transmitted: October 31, 2017
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) 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 FISMA metrics provided by the Department of Homeland Security and the Office of Management and Budget (OMB) in support of OMB Memorandum M-18-02.

Carson found that the CPSC was not compliant with all of FISMA's requirements. However, the CPCS was making progress in implementing many of the FISMA requirements. Carson identified 13 findings and made 46 recommendations to improve the CPSC's information security posture.

AUDIT OF THE CPSC'S COMPLIANCE WITH THE DATA ACT
Transmitted: November 8, 2017
For the full report click here

The Digital Accountability and Transparency Act (DATA Act) established government-wide financial data standards. It also requires federal agencies to report financial and award data in a new website, USASpending.gov. The DATA Act also requires the Inspector General of each federal agency to assess a statistically valid sample of the spending data submitted by its federal agency. The results are submitted to Congress in a publicly available report assessing the completeness, timeliness, quality, and accuracy of the data sampled and the implementation and use of the Government-wide financial data standards by the federal agency. The audit was performed in accordance with generally accepted government auditing standards.

Overall, we found issues with the completeness and accuracy of CPSC information posted to USAspending.gov. We found no timeliness issues. We noted that overall quality was a reflection of government-wide and agency errors. We made two recommendations to help the agency address these findings.

AUDIT OF THE CONSUMER PRODUCT SAFETY COMMISSION'S FISCAL YEAR 2017 FINANCIAL STATEMENTS
Transmitted: November 14, 2017
For the full report click here

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. To conduct this audit, the CPSC OIG contracted with CliftonLarsonAllen, LLP, an independent public accounting firm. The contract required CliftonLarsonAllen to perform an independent audit of the CPSC's financial statements according to generally accepted government auditing standards, OMB Bulletin 17–03, and the President's Council on Integrity and Efficiency/Government Accountability Office's (GAO) Financial Audit Manual, for the periods ended September 30, 2017, and 2016.

Overall, CLA found that the CPSC's financial statements were fairly presented.

Ongoing Projects

REVIEW OF THE CPSC'S COMPLIANCE WITH THE IMPROPER PAYMENTS ELIMINATION AND RECOVERY ACT (IPERA) FOR FY 2017

The OIG contracted with Kearney & Company (Kearney), to perform a review of the CPSC's compliance with the reporting requirements contained in the IPERA, as amended by the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA), for transactions in FY 2017. The review is being performed in accordance with CIGIE's QSIE. The review focuses on the CPSC's compliance with the six elements identified as criteria in OMB's Memorandum M-15-02 for payment accuracy, as well as overall program internal controls.

REVIEW OF THE CPSC'S VENDOR PAYMENTS FOR FY 2017

The control weaknesses identified in the FY 16 IPERA compliance review prompted the OIG to evaluate the CPSC's processes for managing vendor payments. The objective of this review is 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 17. The CPSC OIG contracted with Kearney, to perform this evaluation in accordance with CIGIE QSIE.

AUDIT OF THE OCCUPANT EMERGENCY PROGRAM FOR FY 2017

The OIG is auditing the CPSC's Occupant Emergency Program for fiscal year 2017. The purpose of the 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 is to determine program effectiveness and compliance with the Interagency Security Committee Guide. The audit is being performed in accordance with generally accepted government audit standards.

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

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. To conduct this audit, the CPSC 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 relevant standards, for the periods ended September 30, 2018, and 2017.

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 CPSIA requires the CPSC to implement a publicly accessible, searchable database of consumer product incident reports called the Consumer Product Safety Risk Management System (CPSRMS). The objective of this review was to evaluate the application of the Risk Management Framework to 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.

AUDIT OF THE FEDERAL TRANSIT BENEFITS PROGRAM
Transmitted: March 24, 2014
For the full report click here

The OIG conducted an audit of the Federal Transit Benefits Program (FTBP) at the CPSC. We reviewed FTBP activity at the CPSC for the period October 1, 2011, through December 31, 2012. The objectives of this audit included assessing the adequacy of the CPSC's remediation efforts of findings identified in a 2009 OIG review. This audit was conducted under generally accepted government auditing standards.

We also audited whether internal controls were designed, implemented, and operated effectively to ensure that the FTBP objectives were met and the program complied with relevant laws and regulations. We found the CPSC had a functioning FTBP, but the program had several internal control weaknesses and did not comply with certain policies and procedures mandated by the U.S. Department of Transportation, the CPSC's FTBP service provider.

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 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. The objective was to determine whether the CPSC had established adequate internal controls over employee wage garnishments and appropriate tax withholdings. 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.

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 generally accepted government auditing standards. 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.

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, including fee assessments, for FOIA requests processed between October 1, 2008, and September 30, 2013. The OIG conducted this audit under generally accepted government auditing standards. We found that agency records that are not available to the public through "reading rooms," may be available in response to Freedom of Information Act (FOIA) requests. 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.

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.

AUDIT OF THE GOVERNMENT PURCHASE CARD PROGRAM
Transmitted: March 29, 2017
For the full report click here

The objective of this audit was to assess the CPSC's compliance with laws and regulations over the purchase card program. To that end, we assessed the internal control environment and management's monitoring and administration of the program. The audit was performed in accordance with generally accepted government auditing standards. Overall, we found that the CPSC had made enhancements to the program since our last audit, but work remained to be done. We made nine consolidated recommendations to improve the program.

REPORT ON THE PERFORMANCE REVIEW OVER IPERA PROGRAM FOR CPSC
Transmitted: May 15, 2017
For the full report click here

The objective of this review was to assess the CPSC's compliance with the requirements contained in the IPERA, as amended by the IPERIA, for FY 2016. The OIG contracted with Kearney to perform this review in accordance with CIGIE's 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 three recommendations to improve the program.

PERFORMANCE AUDIT OF INTERNAL CONTROLS OVER CONTRACT MANAGEMENT AND ADMINISTRATION FOR FISCAL YEAR 2016
Transmitted: July 27, 2017
For the full report click here

The OIG contracted with Kearney to audit the CPSC's contract management process. The audit was performed in accordance with generally accepted government auditing standards. 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. We made 14 recommendations to improve CPSC contract management.

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 generally accepted government auditing standards. 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.

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 other concerned individuals. The objective of this program is to ensure 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, 2017, to March 31, 2018.

Investigation Status	Count
Open as of October 1, 2017	3
Opened during reporting period	11
Closed during reporting period	1
Transferred to other Depts./Agencies	8
Referred to Dept. of Justice Criminal Prosecution	0
Referred to State/Local Criminal Prosecution	0
Total Indictments/ Information from Prior Referrals	0
Open as of March 31, 2018	5

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

Reportable Investigations

18-01 Complaint alleged issues with Corrugated Stainless Steel Tubing (CSST) in residences. The complaint was outside the jurisdiction of the OIG and referred to agency management for resolution.

18-02 Complaint alleged issues with a personal computer. The complaint was outside the jurisdiction of the OIG and referred to agency management for resolution.

18-03 Complaint alleged issues with aviation navigation devices. This complaint was outside of the jurisdiction of the OIG and referred to an outside agency for resolution.

18-04 Complaint alleged issues with clothing items not meeting agency standards. This complaint was outside of the jurisdiction of the OIG and referred to Agency management for resolution.

18-05 Complaint alleged possible conflict of interest issues regarding an agency employee. A preliminary inquiry found no evidence of conflict of interest violations and the complaint was closed.

18-06 Complaint alleged issues with childproof caps on liquid camp fuel. This complaint was outside of the jurisdiction of the OIG and referred to agency management for resolution.

18-07 Complaint alleged issues with water quality in state of residence. This complaint was outside of the jurisdiction of the OIG and referred to several outside agencies for resolution.

18-08 Complaint alleged issues with a personal computer. This complaint was outside of the jurisdiction of the OIG and referred to agency management for resolution.

18-09 Complaint alleged issues with the importation of consumer products. After a preliminary inquiry, the complaint was referred to agency management for resolution.

18-10 Complaint alleged issues in the budget reconciliation process. The complaint is currently under investigation.

18-11 Complaint alleged issues regarding flame retardant chemicals used on a mattress. The complaint is currently under investigation.

Other Activities

Legislation and Regulatory Review

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

Administrative Leave Act
Anti-Deficiency Act
Codification of the IG Act at 5 U.S.C. Chapter 4
Conflict of Interest Policies
Consumer Product Safety Act
Consumer Product Safety Improvement Act
Cybersecurity Information Sharing 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
Financial Management Policies
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
Inspectors General Empowerment Act of 2016
IG Recommendation Transparency Act of 2018
NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017
OPM Regulations on Administrative Leave Act
Privacy Program
Prohibited Personnel Practices
Standards of Conduct for Government Employees
Telework Enhancement Act of 2010
Telework Policies
Training of Managers and Supervisors
Whistleblower Ombudsman Reauthorization Bill
Whistleblower Protection Act
Whistleblower Protection Enhancement Act
Whistleblower Right to Know 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 Inspector General regularly attends meetings held by CIGIE and their joint meetings with GAO. The OIG's staff attended seminars and training sessions sponsored or approved by CIGIE.

COUNCIL OF COUNSELS TO THE INSPECTORS GENERAL

The Attorney-Advisor 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 Attorney-Advisor 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.	8-11, 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.	8-11
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.	NA

Appendix B: Peer Review

Generally accepted 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 OIG.

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
CPSIA	Consumer Product Safety Improvement Act of 2008
CPSC	U.S. Consumer Product Safety Commission
CPSRMS	Consumer Product Safety Risk Management System
DATA Act	Digital Accountability and Transparency Act of 2014
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FTBP	Federal Transit Benefits Program
FY	Fiscal Year
GAO	U. S. Government Accountability Office
IG	Inspector General
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 of 2012
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, the CPSC has made substantial progress in closing out earlier recommendations. During the last six month period CPSC management took corrective actions that resulted in the closing of 20 open recommendations. In addition, as a reflection of the changing FISMA metrics, OIG updated the current open FISMA recommendations to reflect the results of the FY 2017 FISMA report.

Report Name and Date	*Consolidated Recommendations*
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.
Audit of the CPSC's Federal Transit Benefits (FTBP) March 24, 2014	FTBP - 1. Modify and publish CPSC Directive 862.1 to comply with the new procedures, current processes, and requirements for the transit benefit program to include, verification of applicant information, routine reviews (at least annually) of participant data, routine reconciliations (at least monthly) of CPSC and FTSB provider records. FTBP - 2. Update and publish procedures for reclaiming transit benefit media from employees who exit FTBP either permanently or temporarily. FTBBP - 3. Train employees and transit program staff on the requirements of the program and provide documentation to support training completion of transit program staff and beneficiaries FTBP - 4. Update CPSC Forms 119 and 119A to reflect current guidance. FTBP – 5. Develop and implement a process to identify beneficiaries on long-term leave and ensure their benefits are blocked while on leave. Further, review transit benefit use of prior long-term leave

Report Name and Date	*Consolidated Recommendations*
	recipients and recover any improperly received benefits.
Evaluation of the CPSC's Dealings with Employee Debt (Debt) September 30, 2014	DEBT - 1. Management develop and document 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 CPSC Third Party Lab 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.
FOIA Program Audit (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 Act Review (Cyber) August 14, 2016	Cyber -1. Management update, develop and publish 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

Report Name and Date	*Consolidated Recommendations*
	contain PII. Cyber - 3. The General Access Control Policy and attendant procedures should be updated to include the elements outlined in the report. Cyber -4. Develop, document, and maintain a software inventory including license management policies and procedures. Cyber – 5. Comply with and enforce HSPD-12 multifactor authentication supported by the Personal Identity Verification Card.
Audit of CPSC's Purchase Card Program (Pcard) March 29, 2017	Pcard – 1. Revise and implement program guidance, including the Handbook and Standard Operating Procedures to align to the current process and reflect current government-wide laws and regulations to include topics such as document retention requirements, split purchases, sales tax regulations, bank issuer document review and approval process. Pcard - 2. Revise and implement the Purchase Card Handbook to properly address and provide guidelines for Cardholders to follow when they are also acting as the FCO. Pcard – 3. Implement a tolerable threshold that the Cardholder may not exceed without obtaining additional Approving Official approval prior to purchase. Pcard – 4. Implement and train cardholders on purchase card program requirements for new cardholders, reviewers, and program officials and regularly, as least annually, provide refresher training both for CPSC specific requirements and bank issuer requirements for all cardholders, approvers, and program officials and document training completion. Pcard – 5. Review and document the results of analysis of cost effectiveness of current of monthly reconciliation procedures and any proposed alternatives. Pcard – 6. Update agency exit procedures to require proof of card return before final employee exit approval. Pcard – 7. Require the APC to obtain independent witness documentation whenever cards are destroyed. Pcard – 8. Develop and implement an effective property management system for accountable property purchased by purchase card. Pcard – 9. Revise and publish guidance for the annual supervisory review of transactions to include random sampling for the testing and provide for independent review of results.
CPSC FY 2016 IPERA Report May 15, 2017	IPERA-1. Develop and implement an effective process for evaluating internal controls as part of the IPERA risk assessment. IPERA-2. Develop and implement CPSC practices, policies, and procedures which comply with the FAR. IPERA-3. Estimate the total amount of improper payments based on the systemic nature of the issue and the longstanding lack of formal delegation of authority. Report the payments as improper and implement the appropriate remediation and CAP depending on the total amount.

Report Name and Date	*Consolidated Recommendations*
CPSC 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-9. Integrate PRISM into the CPSC information technology risk management program. 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.
FY 2017 FISMA 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. FISMA-39. Develop and distribute an organization-wide information security program plan.

Report Name and Date	*Consolidated Recommendations*
	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.
CPSC Compliance with the Digital Accountability and Transparency Act Fiscal Year 2017 (DATA) November 9, 2017	DATA – 1. Develop a review process that ensures the data entered is accurate and reliable before it is submitted to ESC and the data Broker, prior to certification by the SAO. DATA – 2. Establish a process to communicate DATA Act issues to Government-wide providers, to include the Broker, and document those communications.

CONTACT US

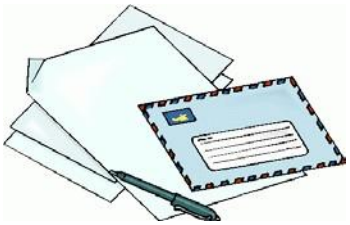
If you want to confidentially report or discuss any instance of misconduct, fraud, waste, abuse, or mismanagement involving CPSC's programs and operations, please contact the CPSC Office of Inspector General.

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