Office of Inspector General

U.S. Consumer Product Safety Commission

Semiannual Report to Congress

April 1, 2017 – September 30, 2017

October 31, 2017

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 the Congress to improve program management;

Maximize the positive impact and ensure the independence and objectivity of our audits, investigations, and other reviews;

Use our investigations and other reviews to increase Government integrity and recommend improved systems to prevent fraud, waste, and abuse;

Be innovative, question existing procedures, and suggest improvements;

Build relationships with program managers based on a shared commitment to improving program operations and effectiveness;

Strive to continually improve the quality and usefulness of our products; and

Work together to address Government-wide issues.

Office of Inspector General
U. S. CONSUMER PRODUCT SAFETY COMMISSION

October 31, 2017

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 April 1, 2017, through September 30, 2017. The 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 (CIGIE) 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 to "Save Lives and Keep Families 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.

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 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.

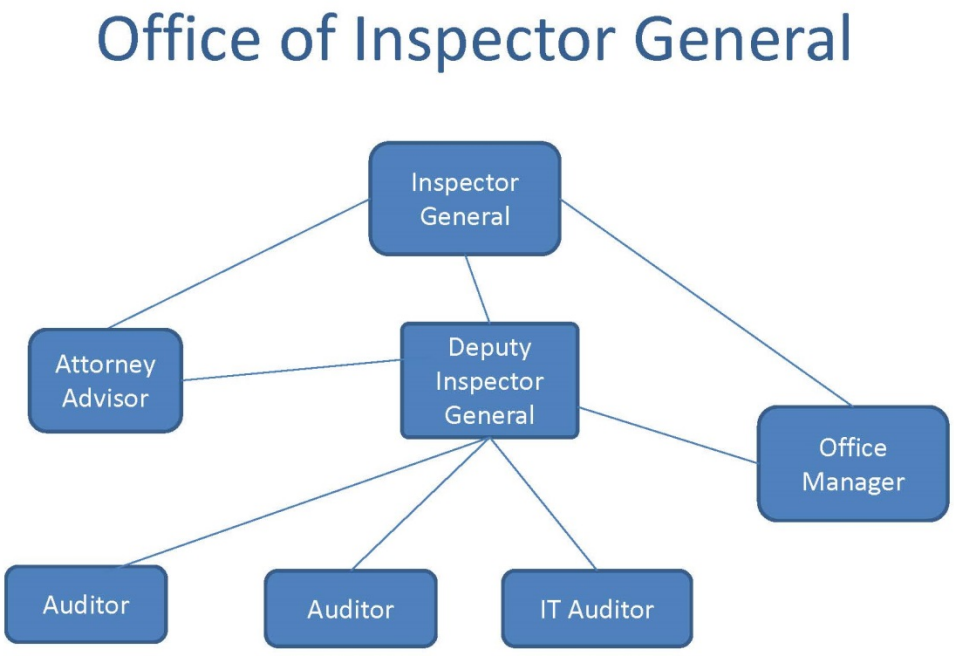
The IG Act gives the Inspector General the authority and responsibility to:

- 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 four audits or reviews. At the end of the reporting period three audits or reviews remained ongoing.

Completed Reports

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

The OIG contracted with Kearney & Co. to perform a review of the CPSC's compliance with the reporting requirements contained in the Improper Payment Elimination and Recovery Act of 2010 (IPERA), as amended by the Improper Payment Elimination and Recovery Improvement Act of 2012, for transactions in Fiscal Year (FY) 2016. The review was performed in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Quality Standards for Inspections and Evaluations. The review focused on the CPSC's compliance with the six elements identified as criteria in Office of Management and Budget's (OMB) Memorandum M-15-02 for payment accuracy, as well as overall program internal controls.

Kearney found that based on the lack of proper delegation of payment authority, all payments authorized by Contracting Officer's Representatives during FY 2016 at the CPSC were improper, as that term is defined for the purposes of IPERA. Kearney determined that the CPSC neither identified nor reported to Congress the resulting improper payments amounting to approximately $29.4 million.

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 & Co. to audit the CPSC's contract management process. The audit was performed in accordance with generally accepted auditing standards. The objective of this engagement was to ascertain whether CPSC had established and implemented effective internal controls to guide its contract/acquisitions management process for its firm-fixed-price contracts and whether the contract monitoring process utilized by CPSC adhered to applicable Federal laws and regulations.

Kearney concluded that the CPSC did not have an effective system of internal controls implemented or operating effectively over its FY 2016 contract management process. Many of the issues that were identified were the result of a lack of adequate or effective policies and procedures. Additionally, the contract monitoring process used by CPSC did not comply with applicable laws and regulations.

AUDIT OF THE FAST TRACK RECALL PROGRAM
Transmitted: September 19, 2017
For the full report click here

The objectives of our audit were to assess the effectiveness of the Fast Track Recall program (Fast Track) in meeting its goals for the CPSC, industry, and consumers, as well as assess compliance with relevant laws and regulations. Specifically, we evaluated whether the CPSC had collected relevant data to determine whether internal controls were adequate and the program was effective; and verified compliance with relevant laws and regulations.

Overall, we found Fast Track was effective in getting unsafe products off the market quickly and efficiently. We also found no instances of non-compliance with applicable laws and regulations. In many cases, a firm had already stopped the sale of a defective product prior to notifying the CPSC. Companies which used the program agreed that the program was effective in getting unsafe products off the market and the CPSC's staff was knowledgeable and helpful. However, we found that with regards to performance measures, not all of the Fast Track case and cost data were being captured.

AUDIT OF THE TELEWORK PROGRAM FOR FISCAL YEAR 2016
Transmitted: September 29, 2017
For the full report click here

The primary 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 its Telework Program in accordance with Federal laws, regulations, guidance, and agency policy.

The CPSC effectively required all teleworkers to have a signed telework agreement prior to beginning telework and developed policies and procedures to govern the agency's Telework Program. However, management did not have adequate internal controls in place to support the agency's Telework Program. The agency's Telework Program was not coordinated with broader agency goals and strategic plans and did not comply with all of the applicable Federal laws and regulations.

Ongoing Projects

FINANCIAL STATEMENT AUDIT FY 2017

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, an independent public accounting firm. The contract requires CliftonLarsonAllen to perform an independent audit of the CPSC's financial statements according to generally accepted auditing standards, OMB Bulletin 15 – 02, 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.

FEDERAL INFORMATION SECURITY MODERNIZATION ACT REVIEW REPORT FOR FY 2017

The Federal Information Security Management Act of 2002 (FISMA), as amended by the Federal Information Security Modernization Act of 2014, requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. OMB uses this data to assist in its oversight responsibilities and to prepare an annual report to Congress on agency compliance with FISMA. To conduct this review, the CPSC OIG contracted with Carson, Inc., a management consulting firm to complete the review in accordance with the CIGIE Quality Standards for Inspections and Evaluations.

FY 2017 DATA ACT REVIEW

The Digital Accountability and Transparency Act (DATA Act), in part, requires Federal agencies to report financial and award data in accordance with the established Government-wide financial data standards in a new website, USASpending.gov. The DATA Act also requires the IG of each Federal agency to review a statistically valid sample of the spending data submitted by its Federal agency and to submit to Congress a publicly available report assessing the completeness, timeliness, quality, and accuracy of the data sampled and the implementation and use of the Government-wide financial data standards by the Federal agency.

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. 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 issues identified in a 2009 OIG review. 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.

FOLLOW-UP AUDIT OF THE CPSC'S INFORMATION TECHNOLOGY INVESTMENT MANAGEMENT
Transmitted: May 20, 2014
For the full report click here

The OIG conducted a follow-up performance audit related to the CPSC's Information Technology Investment Management (ITIM) processes, using GAO's ITIM framework. The audit objectives were to determine where the CPSC was on the GAO ITIM maturity model. Two prior audits indicated the CPSC was at level one. We found the

CPSC was still at level one, but had reduced the number of open recommendations from eleven to five.

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 an evaluation 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. 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 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.

CPSC'S COMPLIANCE WITH THE GOVERNMENT PERFORMANCE AND RESULTS ACT, AS AMENDED, AND THE RELIABILITY OF ITS PUBLISHED FY2013 PERFORMANCE DATA
Transmitted: December 15, 2014
For the full report click here

The OIG conducted a performance audit of the CPSC's compliance with the Government Performance and Results Act, as amended, and Government Performance and Results Modernization Act of 2010 and over the reliability of its published FY 2013 Performance Data. We found the CPSC had made significant progress in its implementation of Government Performance and Results Modernization Act of 2010 requirements, especially compliance with revised reporting requirements. However, while we found some policies and procedures had been developed, lack of full implementation hindered the agency's ability to validate the accuracy and reliability of the performance data reported in the CPSC's FY 2013 Annual Performance Report.

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

The OIG conducted this audit to assess the adequacy of the CPSC's procedures for accrediting laboratory assessment bodies. 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 COLLECTION OF CIVIL PENALTIES
Transmitted: August 3, 2015
For the full report click here

One way the CPSC holds violators accountable for hazardous consumer products is by using its civil penalty authorities. The CPSIA of 2008 provided the CPSC with significant new regulatory and enforcement tools including enhanced civil penalties. Companies which knowingly fail to report potentially hazardous products, as required, can be subject to civil penalties. Our audit covered civil penalty collection transactions for the period October 1, 2011, through September 30, 2014. We found the CPSC had a functioning Civil Penalty Collection Program, but the program had several internal control weaknesses and did not comply with certain contract provisions.

AUDIT OF THE FREEDOM OF INFORMATION ACT PROGRAM
Transmitted: September 30, 2015
For the full report click here

Agency records that are not available to the public through "reading rooms," may be available in response to Freedom of Information Act (FOIA) requests. Our audit was to determine whether the CPSC had developed proper internal controls, 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. We found that the CPSC had a functioning program, but 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 purpose of our 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. 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.

FY 2016 FEDERAL INFORMATION SECURITY MANAGEMENT ACT REVIEW REPORT
Transmitted: December 14, 2016
For the full report click here

FISMA, as amended by the Federal Information Security Modernization Act of 2014, requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. OMB uses this data to assist in its oversight responsibilities and to prepare an annual report to Congress on agency compliance with FISMA. The review was performed in accordance with the CIGIE Quality Standards for Inspections and Evaluations. We found the CPSC had made progress in implementing FISMA requirements, but work remained to be done.

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

The objective of the audit was to assess the CPSC's compliance with laws and regulations over the purchase card program, as well as the internal control environment, and management's monitoring and administration of the program. The audit was performed in accordance with Generally Accepted Auditing Standards. Overall, we found that the CPSC had made enhancements to the program since our last audit, but work remained to be done.

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 actionable investigations involving a senior Government employee nor did the OIG receive any actionable allegations of whistleblower retaliation. The table below summarizes the disposition of complaint and investigative work performed from April 1, 2017 to September 30, 2017.

Investigation Status	Count
Open as of April 1, 2017	1
Opened during reporting period	5
Closed during reporting period	0
Transferred to other Depts./Agencies	3
Referred to DOJ Criminal Prosecution	0
Referred to State/Local Criminal Prosecution	0
Total Indictments/Information from Prior Referrals	0
Open as of September 30, 2017	3

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

Reportable Investigations

17-08 Complaint alleged whistleblower retaliation for a federal contractor at another agency. The complaint was referred to the Office of Special Counsel.

17-09 Complaint alleged issues with the standards governing playground slides. The complaint was outside the jurisdiction of the OIG and referred to Agency management for resolution.

17-10 Complaint alleged issues with counterfeit children's jewelry. This complaint was outside of the jurisdiction of the OIG and referred to Agency management for resolution.

17-11 Complaint alleged fraud in the Saferproducts.gov reporting process. This complaint is currently under investigation.

17-12 Complaint alleged issues with employee misuse of a government vehicle. This 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
ALB17705 Increase Transparency of IG Budget Request
Anti-Deficiency Act
Conflict of Interest Policies
Consumer Product Safety Act
Consumer Product Safety Improvement Act
Cybersecurity Information Sharing Act
Digital Accountability and Transparency Act
Ethics Regulations
Every Dollar Counts Act
Federal Acquisition Regulations
Federal Information Security Modernization Act
Federal Records Modernization Act of 2016
Federal Travel Regulations
Financial Management Policies
Freedom of Information Act
Government Charge Card Abuse Prevention Act
Government Performance and Results Act
Grants Oversight and New Efficiency Act
Hatch Act
H.R. 2196
IG Access to Contractor/Grantee information
Improper Payments Elimination and Recovery Improvement Act
Inspector General Act, as amended
Inspectors General Empowerment Act of 2016
NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017
OPM Regulations on Administrative Leave Act
Payment of Credentials (5 U.S.C. 5757)
Privacy Program
Prohibited Personnel Practices
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.	14-15
Section 5(a)(1)	Significant problems, abuses, and deficiencies.	5-6, 8-11
Section 5(a)(2)	Recommendations with respect to significant problems, abuses, and deficiencies.	5-6, 8-11
Section 5(a)(3)	Prior significant recommendations on which corrective action has not been completed.	8-11, 19-28
Section 5(a)(4)	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, 8-13
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, 19-28
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	
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	Government Accountability Office
IG	Inspector General
IG Act	The Inspector General Act of 1978, as amended
IPERA	Improper Payments Elimination and Recovery Act
ITIM	Information Technology Investment Management
OIG	Office of Inspector General
OMB	Office of Management and Budget

Appendix D: Consolidated List of Open Recommendations

During this reporting period, the OIG reviewed the open recommendations as originally published within individual reports. We have consolidated some recommendations. For example, multiple recommendations regarding training within a report have been combined into a single training recommendation.

Report Name	*Consolidated Recommendations*	*Report Date*
Risk Management System - Information Security Review Report (RMS)	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 POAM to include the missing information, as required by OMB M-4-25 RMS-5. Perform an assessment to ensure the adequate categorization of information types	6/5/2012
Audit of the CPSC's Federal Transit Benefits (FTBP)	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. FTBP-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 recipients and recover any improperly received benefits.	3/24/2014
OIG Performance Audit of Information Technology	ITIM-1. Enforce the requirements of the IRB charter to include meeting schedule, document meeting deliberations	5/20/2014

Report Name	*Consolidated Recommendations*	*Report Date*
Investment Management (ITIM)	and decisions, including alignment of information technology investments to CPSC strategic goals and objectives.	
Evaluation of the CPSC's Dealings with Employee Debt (Debt)	DEBT-1. 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. Develop a process to regularly, at least annually, review employee exemption and withholding status for reasonableness.	9/30/2014
GPRA Final Audit Report 2014 (GPRA)	GPRA-1. Establish and document verification and validation techniques that will ensure the completeness and reliability of all performance data included in CPSC's Annual Performance plans and reports as appropriate to the intended use of the data.	12/15/2014
FY 2013 CPSC Third Party Lab Accreditation Program Performance Audit (Lab)	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.	2/23/2015
Civil Penalties Program Audit (Civil)	Civil-1. Develop, and implement policies and procedures documenting roles, responsibilities related to distribution of settlement notices, establishing civil penalty receivables in the financial system, recording, and reconciling penalty payment information, including late payments, and closing completed settlement agreements. Civil-2. Provide training to all staff who work establishing, collecting, and closing civil penalty settlement notices, relevant to their area of responsibility. Provide documentation indicating who has completed the initial training. Civil-3. Coordinate payment terms to reflect the requirements of CPSC and Department of the Treasury financial systems.	8/3/2015
FOIA Program Audit (FOIA)	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-2. Develop and implement an annual training and development program for all agency employees involved with requests associated with the CPSC FOIA Program, including program analysts who work with clearinghouse data. The training should include education on the FOIA, the CPSC's FOIA procedural requirements/internal controls, and when and how to properly assess fees for FOIA records.	9/30/2015

Report Name	Consolidated Recommendations	Report Date
	FOIA-3. Develop and implement an SOP consistent with current FOIA legislation related to receipt, processing, and tracking of FOIA requests for IDI files. FOIA-4. Log all FOIA requests received into the FOIAXpress system or similar non-electronic system where information is retrievable. FOIA-5. Develop and implement a record retention schedule that complies with all current document retention requirements. FOIA-6. Develop and implement an effective FOIA monitoring system to measure timeliness of completion of all FOIA requests within statutory deadlines and whether they should be assessed fees. FOIA-7. Develop and implement a training program for all staff involved in FOIA fee collection and reconciliation including late payments and closing completed payment agreements for accurate financial reporting. 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. Review and publish an updated fee schedule regularly, at least annually. FOIA-10. Develop and implement 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. Document a review of the data fields in FOIAXpress for accuracy, completeness, and timeliness.	
Cybersecurity Act Review (Cyber)	Cyber-1. Update and implement general access control and logical access control policies and procedures for all systems that permit access to PII. Cyber-2. Train or document training completion by individual system owners on establishing, implementing, and maintaining logical access policies and procedures for systems that contain PII. Cyber-3. Update the General Access Control Policy and attendant procedures 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.	8/14/2016
FY 2016 Federal Information Security Management Act Evaluation (FISMA)	**Risk Management** FISMA-1. Define and implement the Risk Management/ISCM policy/procedures/strategies in accordance with NIST requirements.	12/14/2016

Report Name	Consolidated Recommendations	Report Date
	FISMA-2. Perform a Gap Analysis to identify the missing knowledge, skills, and abilities required to implement the ISCM program and remediate accordingly. FISMA-3. Document and certify a complete systems inventory that includes all CPSC systems (both major and minor systems), and include a description of each system in this systems inventory. FISMA-4. Review and certify the inventory of all systems annually, and in the event of a major change. FISMA-5. Categorize each of the agency's systems (including all of the CPSC's minor applications), and select, implement, and assess the security controls employed by each of these systems. FISMA-6. Formally authorize the operation of each agency system, including the agency's minor systems. FISMA-7. Update existing security plans to describe how all of the selected security controls are implemented. FISMA-8. Update the existing security plans, where applicable, to include a description of all agency systems and data types, and include a description of how the controls selected for each of the minor applications are implemented. FISMA-9. Perform and document a formal assessment to categorize all agency systems based on the NIST SP 800-60 guidance. FISMA-10. Document all of the OMB M 04-25 required information for all security weaknesses tracked in the agency POAMs. FISMA-11. Document a comprehensive risk assessment for the Drupal implementation in accordance with NIST guidance. **Continuous Monitoring** FISMA-12. Define the responsibilities for all ISCM stakeholders and communicate this information to those resources. FISMA-13. Perform and maintain a Gap Analysis to identify the missing knowledge, skills, and abilities required to implement the ISCM program. FISMA-14. Develop and implement a remediation plan for each of the shortfalls noted in the ISCM Gap Analysis. FISMA-15. Clearly describe the methodology used to calculate the organizational risk tolerance, include this description in the Organization-Wide Risk Management Strategy and integrate this methodology into the ISCM Strategy. FISMA-16. Formally define and implement a process that facilitates consistently capturing and sharing the lessons learned related to the effectiveness of ISCM processes and activities.	

Report Name	Consolidated Recommendations	Report Date
	FISMA-17. Identify, fully define, and develop a plan for implementing the ISCM technologies management expects to utilize. **Contingency Planning** FISMA-18. Develop and implement an FCD1 compliant TT&E program. FISMA-19. Update the contingency planning policy and develop and implement procedures to meet NIST, FCD1, and NARA requirements: FISMA-20. Establish, document, test, and approve a DR Plan, BCP, and COOP and document appropriate lessons learned and after action reports. FISMA-21. Perform, document, and approve a formal BIA in accordance with NIST SP 800-34. FISMA-22. Establish, formalize, test, and approve ISCPs for all critical agency systems in accordance with FEMA, NIST, and NARA guidance. FISMA-23. Establish an Alternative Processing Site. FISMA-24. Train all relevant resources on the continuity planning responsibilities assigned to them in the policy. FISMA-25. Implement a solution to allow management to meet the documented RPOs for all relevant systems. **Contractor Systems** FISMA-26. Develop a formal process to ensure that all requisite FAR clauses and security information is included in contracts/agreements moving forward. FISMA-27. Establish coordination between the Division of Procurement Services (FMPS), Office of the General Counsel (OGC), and the Office of Information Technology (EXIT) to ensure that all of the recommendations outlined in the CAO's Best Practices for Acquiring IT as a Service are incorporated into agency policies, procedures, practices, and third-party agreements. FISMA-28. Update the Contractor Oversight Policies and develop attendant Procedures to include the following meet FISMA requirements. FISMA-29. Establish and implement processes and procedures to ensure all connecting systems meet FISMA requirements. **Configuration Management** FISMA-30. Update the Configuration Management policies, and develop and implement SOPs to standardize the implementation of the Configuration Management process and meet NIST requirements. FISMA-31. Develop, document, and implement a configuration management plan for agency information systems.	

Report Name	Consolidated Recommendations	Report Date
	FISMA-32. Develop, document, and maintain under configuration control baseline configurations for all system components. FISMA-33. Develop and maintain a comprehensive inventory of software and hardware. FISMA-34. Employ automated mechanisms to actively detect hardware devices and software on the network. FISMA-35. Update the Risk Assessment policies/procedures to require the patching of critical agency systems within 30 days in accordance with OMB M 16-04 and to meet NIST requirements FISMA-36. Implement client, server, database and third-party patches in a timely manner. FISMA-37. Test all client, server, database, and third-party patches in a test environment prior to deploying the patch to the full production domain and document the steps taken to test patches in the change control forms. FISMA-38. Add a separate query to the change management database to allow users to search on server, database, and third-party patches. FISMA-39. Upgrade to a supported versions of the existing Operating Systems, databases, and third-party applications. FISMA-40. Scan Sybase databases and websites for patch compliance. **Incident Response and Reporting** FISMA-41. Update and implement the IR Policy, Plan, and Procedures to meet NIST and US-CERT requirements. FISMA-42. Disseminate the IR Policy/Plan to all users with CSIRT supporting roles documented in the respective policy/plans. FISMA-43. Perform and maintain a Gap Analysis to identify the missing skills, knowledge, and resources required to implement the IR program. FISMA-44. Develop and implement a remediation plan for each of the shortfalls noted in the IR Gap Analysis. **Security Training** FISMA-45. Update the Security Training Policy and develop a 5 C.F.R 930.301 compliant training program, using the guidance outlined in NIST SP 800-16 and NIST SP 800-50. FISMA-46. Assign all applicable agency resources to one (or more) of the relevant “user groups” required by NIST SP 800-16/50 and C.F.R 903.301 and provide those resources with the associated training. FISMA-47. Establish and implement a formal policy to require	

Report Name	Consolidated Recommendations	Report Date
	specialized privacy training for all users with significant privacy responsibilities. FISMA-48. Perform a gap analysis to identify missing skills, knowledge, and abilities of individuals with significant security and privacy responsibilities and develop and implement a remediation plan for all shortfalls identified. FISMA-49. Develop measures/metrics (based on the NIST SP 800-55 guidance) to assess CPSC user security and privacy awareness against and formalize those measures/metrics in CPSC policies and procedures. FISMA-50. Implement an automated solution to perform attack simulations. FISMA-51. Monitor and report the results of the new measures/metrics and the attack simulations used, to identify future training opportunities. **Identity and Access Management** FISMA-52. Implement the Principle of Least Privilege and establish proper segregation of duties for the GSS. FISMA-53. Systematically compel PIV card authentication for all users accessing CPSC systems. FISMA-54. Implement a formal process to identify, limit and control the use of shared user accounts. FISMA-55. Develop and implement logical access control policies and procedures for all agency systems that meet NIST requirements. FISMA-56. Provide training to individual system owners, where necessary, on how to establish, implement, and maintain logical access policies and procedures. FISMA-57. Implement a network access control solution to authenticate devices prior to allowing access to the network. FISMA-58. Systematically restrict split tunneling. FISMA-59. Perform security scans on devices connecting to the CPSC network prior to allowing access to the network. FISMA-60. Revoke separated users' access to CPSC facilities and all relevant information systems. FISMA-61. Implement a centralized contractor database with automated workflow to track the on and off boarding of contractors. FISMA-62. Draft and implement an SOP that clearly defines the roles and responsibilities for all resources responsible for processing contractor separations. FISMA-63. Configure CPSRMS to revoke accounts after 30 days of inactivity. FISMA-64. Train the Contracting Officer Representatives (CORs), EXRM, and EXIT resources responsible for processing	

Report Name	Consolidated Recommendations	Report Date
	contractor separations on their respective contractor separation responsibilities. FISMA-65. Require a periodic review of contractor status by the CORs and coordinated by EXRM or Procurement; and FISMA-66. Provide the EXIT representatives and the relevant program officials with a weekly report of contractor separations. The agency should formally reconcile the current separations, as indicated on the weekly EXRM contractor separation report, to all the CPSC IT system Access Control Lists to ensure the timely revocation of all user accounts.	
Audit of CPSC's Purchase Card Program (Pcard)	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, at 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 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.	3/29/2017
CPSC FY 2016 IPERA Report	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	5/15/2017

Report Name	Consolidated Recommendations	Report Date
	payments as improper and implement the appropriate remediation and CAP depending on the total amount.	
CPSC Report on the Performance Audit of Internal Controls over Contract Management and Administration for Fiscal Year 2016 (Contracts)	Contracts-1. Update CO warrants to include specific responsibilities, such as the authority to delegate. Contracts-2. Establish COR delegation letters that specifically identify COR rights and responsibilities. These letters should be specific to the contract, signed by both CO and COR, and provided to the contractor. These letters should be maintained in the contract file and be available for inspection and review. 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-4. Offer training to COs on providing effective oversight of COR contract administration. Contracts-5. Develop an effective risk assessment process which identifies, analyzes, and responds to all self-identified risks in the procurement process. Contracts-6. Review all agency procurement policies against the requirements of the FAR and update policies to confirm that CPSC procurement policies implement or supplement the FAR. Contracts-7. Provide regular training, at least annually, to all COs on the FAR documentation requirements. 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-10. Develop and implement tools, templates, policies, and procedures related to effective communication between COs and CORs to use during contract administration. Contracts-11. Develop and provide training on the tools, templates, policies, and procedures for COs and CORs developed in the prior recommendation. 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. Contracts-13. Provide training to COs and specialists on inputting data and evaluating the accuracy of the data. Contracts-14. Evaluate the most effective placement of FMPS, to include the relationship between FMPS staff and the Chief Acquisition Officer, and document the results of the evaluation.	7/25/2017

Report Name	*Consolidated Recommendations*	*Report Date*
Audit of the Fast Track Recall Program (Fast Track)	Fast Track-1. Develop and use a reliable, easy-to-use methodology to calculate and report the percentage of Fast Track cases meeting the agency's performance metrics and ensure that all cases are included. Fast Track-2. Develop and implement a methodology to ensure all relevant Fast Track cost data is being captured and is available to management for monitoring and planning purposes.	9/19/2017
Audit of the Telework Program for Fiscal Year 2016 (Telework)	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. Telework-7. Perform an assessment to identify and remediate all unencrypted laptops currently issued by the CPSC. Telework-8. Implement a formal periodic review of agency laptops to ensure that each CPSC machine is adequately encrypted. Telework-9. Require the staff responsible for encrypting CPSC laptops to formally certify that these machines are adequately encrypted prior to issuance.	9/29/2017

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