



**U.S. Consumer Product Safety Commission  
OFFICE OF INSPECTOR GENERAL**



## **Semiannual Report to Congress**

April 1, 2024 to September 30, 2024

October 30, 2024

25-O-02



## Top 10 Most Significant Open Recommendations from the Office of Inspector General to the U. S. Consumer Product Safety Commission

1.	Develop and implement an internal control system covering the operations of the CPSC's programs. (FMFIA)
2.	Develop and implement a succession plan that conforms to current OPM guidance, to ensure continuity of operations and avoid the loss of critical knowledge. (HCPA)
3.	Develop and implement an Enterprise Risk Management (ERM) program to allow agency officials to utilize risk management principles in the operations of the agency. (FISMA21)
4.	Ensure that management officials are aware of OIG recommendations that impact their areas of responsibility and actively work toward implementing said recommendations. (BREACH)
5.	Develop and implement a data-driven methodology to measure the Human Capital Program's effectiveness and report results to agency management. (HCPA)
6.	Ensure an appropriate complement of resources are in place in relevant financial process areas to manage accounting and reporting matters as they arise. (FSA23)
7.	Use all available tools to assist in the recruitment and retention of staff, particularly in hard to fill positions. (HCPA)
8.	Develop and implement written guidance governing the CPSC's use of statements of assurance to meet its requirements under the FMFIA. (BREACH)
9.	Develop, document, and maintain a software inventory. (CYBER)
10.	Assess the IT security risks previously identified and develop a corrective action plan that prioritizes addressing the most critical risks and establishes a timeline for taking corrective action. (FISMA21)



## MESSAGE FROM THE INSPECTOR GENERAL



I am pleased to submit the Semiannual Report to Congress for the U.S. Consumer Product Safety Commission (CPSC) Office of Inspector General (OIG). This report details the work of the OIG in the oversight of the CPSC for the second half of Fiscal Year (FY) 2024.

My professional and dedicated staff continue to do the work necessary to fight fraud, waste, and abuse at the CPSC while continuing to make findings and recommendations to aid the agency in achieving its mission. Their efforts have been complicated by our being short-staffed. Unfortunately, agency management has prevented us from filling a vacant position and recently proposed reducing OIG authorized staff. This reduction would reduce our staffing level, established in consultation with Congress after the passage of the Consumer Product Safety Improvement Act, below that necessary to provide robust oversight of the activities of the Commission. If this office had the budgetary independence called for in the Inspector General Act, we could determine how best to make any necessary cost savings. Earlier this year, we submitted our second independent budget request. It is my belief that if we received an explicit ear mark in the CPSC's budget, it would aid in resolving the issue of OIG staffing levels and promote our independence.

On a more positive note, I am pleased to report that the agency has continued to make progress toward integrating enterprise risk management into its operations. Although we have not yet had the opportunity to audit management's assertion that it has performed risk assessments and developed formal internal control programs in accordance with federal standards for the 14 offices with core processes that support the CPSC's mission, it is apparent that agency management has placed both emphasis on and resources behind this effort that had been lacking in the past.

Another area where the agency has shown improvement involves their system of directives. A longstanding fundamental weakness in the CPSC's internal control system had been the failure to develop and maintain an up-to-date set of written policies and procedures. As previously reported, sufficient progress has been made in this area so that it has been removed from our Top 10 List of Recommendations for the agency. However, as found in the PIIA assessment, a number of areas of agency operations continue to function with no or out-of-date policies and procedures.

As detailed in the two assessments issued this reporting period, the agency continues to face challenges related to financial operations and IT security. As previously reported in the FY 2023 Financial Statement Audit, internal controls over financial operations, an area which had previously been a strength at the agency, continued to be a weakness. The FY 2023 PIIA assessment found that the CPSC failed to comply with mandatory reporting requirements related to improper payments because the CPSC had neither sufficient payment integrity reporting policies and procedures nor sufficient resources in place to ensure the required information for the OMB Annual Data Call was submitted before the October deadline. Similarly, the FY 2024 FISMA evaluation determined that, despite improvements in a number of areas, the CPSC still had not implemented an effective information security program in accordance with FISMA requirements. The primary reason for this was the CPSC's not taking a formal approach to information security risk management and not prioritizing addressing FISMA requirements and OIG recommendations despite multiple reports urging it to do so.

We look forward to continuing to work with Congress and agency management in order to promote the efficiency and effectiveness of agency programs.

Christopher W. Dentel, Inspector General

## Table of Contents

---

### Contents

BACKGROUND	2
U.S. Consumer Product Safety Commission	2
Office of Inspector General	2
Ongoing Projects	4
AUDIT PROGRAM	5
INSTANCES OF CPSC INTERFERENCE WITH OIG INDEPENDENCE	7
OTHER ACTIVITIES	8
Legislation and Regulatory Review	8
Management Alert	9
OIG Coordination	10
Peer Reviews	11
APPENDIX A: CROSS-REFERENCE TO REPORTING REQUIREMENTS OF THE IG ACT	12
APPENDIX B: STATEMENT REGARDING PLAIN WRITING	13
APPENDIX C: STATUS OF RECOMMENDATIONS	14
The Good Accounting Obligation in Government Act	14
Previously Issued Reports with Open Recommendations	16



## BACKGROUND

---

### **U.S. Consumer Product Safety Commission**

The U.S. Consumer Product Safety Commission (CPSC or Commission) is an independent federal regulatory agency, created in 1972, by the Consumer Product Safety Act (CPSA). In addition to the CPSA, as amended by the Consumer Product Safety Improvement Act of 2008 (CPSIA), and Public Law No. 112-28, the CPSC administers other laws, such as: the Flammable Fabrics Act, the Refrigerator Safety Act, the Federal Hazardous Substances Act, the Poison Prevention Packaging Act, the Labeling of Hazardous Art Materials Act, the Child Safety Protection Act, the Virginia Graeme Baker Pool and Spa Safety Act, the Children's Gasoline Burn Prevention Act, the Drywall Safety Act, the Child Nicotine Poisoning Prevention Act, the Portable Fuel Container Safety Act, the Nicholas and Zachary Burt Memorial Carbon Monoxide Poisoning Prevention Act, the Safe Sleep for Babies Act, Reese's Law, the imitation firearms provisions of Public Law Nos. 100-615 and 117-167, and the Stop Tip-overs of Unstable, Risky Dressers on Youth requirements of Public Law No. 117-328.

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 CPSA and the CPSIA, as well as numerous other laws.

By statute, the CPSC is headed by five commissioners who are nominated by the president and appointed by and with the advice and consent of the Senate. One of the commissioners is designated by the president and confirmed by the Senate to serve as the Chairman of the CPSC. The chairman is the principal executive officer of the Commission. Currently, the commission consists of a full complement of commissioners.



## Office of Inspector General

The Office of Inspector General (OIG) is an independent office established under the provisions of the Inspector General Act of 1978 (IG Act), as amended. The CPSC OIG was established on April 9, 1989. Mr. Christopher W. Dentel was named Inspector General in 2004.

We are agents of positive change striving for continuous improvements in our agency's management and program operations, as well as within the Office of Inspector General.

We are committed to:

- Working with the Commission and the Congress to improve program management.
- Maximizing the positive impact and ensuring the independence and objectivity of our audits, investigations, and other reviews.
- Using our investigations and other reviews to increase government integrity and recommend improved systems to prevent fraud, waste, and abuse.
- Being innovative, questioning existing procedures, and suggesting improvements.
- Building relationships with program managers based on a shared commitment to improving program operations and effectiveness.
- Striving to continually improve the quality and usefulness of our products.
- Working together to address government-wide issues.

We offer actionable recommendations to increase the efficiency and effectiveness of the CPSC in its mission to protect the public against unreasonable risks of injuries associated with consumer products. We focus our available resources on high-risk areas and continuously seek ways to provide value to our stakeholders.

### Top Management and Performance Challenges Facing the CPSC for FY 2025

1. Enterprise Risk Management
2. Resource Management
3. Information Technology  
Security

Due to improvements in the agency's internal control program, the top management challenges facing the CPSC have changed since FY 2024.

We have recently revised our Top Ten Recommendations for the agency to better reflect current Management Challenges.



## Ongoing Projects

As of the date of this report, the OIG has five ongoing projects. These include three discretionary audits. The audits of the agency's import surveillance and third-party laboratory accreditation programs will assess the effectiveness of two CPSC programs that are key to protecting American consumers from dangerous imported products. The third audit is to determine if the CPSC has effective controls over the utilization of its leased space and is complying with relevant laws and regulations. These audits are being performed by CPSC OIG staff. In addition, there is a Management Alert in process. Management alerts are projects which arise as part of OIG's ongoing oversight of agency operations. Finally, the mandatory annual financial statement audit is on-going.

The OIG uses contractors for the statutorily required annual audits. These include the financial statement audit, Federal Information Security Modernization Act (FISMA) evaluation, and Payment Integrity Information Act (PIIA) evaluation. The three contracted engagements address government-wide requirements for which there are a large number of competent contractors available to perform the work. As a result of contracting these assessments out, the OIG is able to focus its resources and leverage the expertise of our staff auditors, who are familiar with the CPSC's mission and programs, on CPSC-specific audits.



## AUDIT PROGRAM

---

During this semiannual period, the OIG completed two audits, reviews, or special projects.

### **Evaluation of the CPSC's Compliance with PIIA for FY 2023 (PIIA 23)**

Transmitted: May 9, 2024

For the full report and list of open recommendations click [here](#).

The OIG contracted with KPMG LLP (KPMG) to perform a review of the CPSC's compliance with the reporting requirements contained in the PIIA, for transactions in FY 2023. The review was performed in accordance with Council of Inspectors General for Integrity and Efficiency (CIGIE) *Quality Standards for Inspection and Evaluation* (QSIE). The review focused on the CPSC's compliance with the elements identified as criteria in the relevant Office of Management and Budget (OMB) guidance, as well as program internal controls. Overall, KPMG found that for FY 2023, the CPSC did not comply with one of four requirements of the PIIA. In accordance with OMB, all elements must be complied with in order to result in overall compliance. KPMG made two recommendations to improve the integrity of CPSC's payment information. One recommendation has already been closed.

### **Evaluation of the CPSC's FISMA Implementation for FY 2024 (FISMA 24)**

Transmitted: July 30, 2024

For the full report and list of open recommendations click [here](#).

The OIG contracted with Williams, Adley & Company-DC, LLP (Williams Adley) to review the CPSC's compliance with the reporting requirements of the FISMA for FY 2024. The objective of this review was to determine the effectiveness of the CPSC's information security program in accordance with the FY 2024 FISMA reporting requirements, issued by the Department of Homeland Security and OMB Memorandum (M)-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*. As a result of recent changes in OMB requirements, this year was the third year under the new continuous monitoring model. Therefore, Williams Adley reviewed only the subset of 37 metrics that were in scope for FY 2024. The review was performed in accordance with CIGIE QSIE.

Williams Adley found that the CPSC was not compliant with all of FISMA's requirements. However, the CPSC was making progress in implementing many FISMA requirements. Williams Adley made 35 recommendations, 3 of which were new, to improve the CPSC's information security posture.





## INVESTIGATIVE PROGRAM

The OIG investigates complaints and information received from the CPSC's employees, other government agencies, and members of the public concerning possible violations of laws, rules, and regulations, as well as claims of mismanagement, abuse of authority, and waste of funds. The objectives of this program are to maintain the integrity of the CPSC and ensure individuals of a fair, impartial, and independent investigation.

Several individuals contacted the OIG directly during the reporting period to discuss their concerns about matters involving CPSC programs and activities. The OIG did not receive any actionable allegations of whistleblower retaliation. The table below summarizes the disposition of complaints and investigative work performed from April 1, 2024, through September 30, 2024.

Investigation Status	Count
Open as of April 1, 2024	1
Opened during reporting period	102
Closed during reporting period	71
Transferred to other Departments/Agencies	26
Investigative Reports issued	0
Referred to Department of Justice for Criminal Prosecution	0
Referred for State/Local Criminal Prosecution	0
Total Indictments/Information from Prior Referrals	0
Open as of September 30, 2024	6

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

No significant investigations, no allegations of misconduct involving a senior government official, and no convictions resulted from investigations conducted by the OIG.



## **INSTANCES OF CPSC INTERFERENCE WITH OIG INDEPENDENCE**

---

The IG Act specifies that Offices of Inspector General are to be independent of the agencies for whom they provide oversight. However, CPSC management continues to insist that they have the authority to interfere in the operations of our office by interjecting themselves into our hiring decisions and reducing our resources. They have cut our authorized staff level without consultation.

Agency management is currently requiring that we receive their permission, through a critical vacancy process, to hire staff. This has resulted in agency management attempting to influence the organization and staffing of our office. This would in and of itself constitute an infringement on our office's statutorily required independence. However, agency management has gone further by repeatedly refusing to authorize us to fill a currently vacant position. The IG Act explicitly grants Inspectors General the authority to hire their staff. Even if management ultimately concurred with the Inspector General's staffing decisions, by requiring their concurrence in our staffing decisions they still risk creating the appearance that this office lacks independence from agency management.

The current proposed CPSC Operating Plan, not yet approved, would affirmatively reduce OIG authorized staff. Although acknowledging that the agency is facing budgetary constraints, asking this office which comprises approximately 1.4 percent of agency staff to provide 9 percent of the necessary reductions does not seem equitable. This is particularly true when other offices are staffed above their authorized levels.

If this office had the budgetary independence called for in the IG Act, we could determine how best to make any necessary cost savings. Earlier this year, we submitted our second independent budget request. It is my belief that if we received an explicit earmark in the CPSC's budget, it would aid in resolving the issue of OIG staffing levels and promote our independence.



## 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:

Antideficiency Act  
American Rescue Plan Act  
CARES Act  
Civil Rights Act of 1964  
Consolidated Appropriations Act 2021 and 2022  
Consumer Product Safety Act  
Consumer Product Safety Commission Regulations  
Consumer Product Safety Improvement Act of 2008  
Economy Act  
Ethics Regulations  
Executive Order 13932  
Executive Order 14035  
Federal Acquisition Regulations  
Federal Travel Regulations  
Freedom of Information Act  
General Services Administration Leasing Regulations  
General Services Administration Personal Property Regulations  
Hatch Act  
Identity Theft and Assumption Deterrence Act  
Inspector General Act of 1978, as amended  
National Defense Authorization Act for Fiscal Year 2023  
Office of Management and Budget Circulars and Memoranda  
Office of Personnel Management Classification Standards



Peer Review Guides  
Privacy Program  
Prohibited Personnel Practices  
Public Buildings Act of 1959  
Public Disclosure of Information, 15 U.S.C. 2055  
Quality Standards for Inspection and Evaluation  
Records Management Policies and Regulations  
Standards of Conduct for Government Employees  
Whistleblower Protection Enhancement Act

## **Management Alerts**

### **Management-Alert-24-M-02**

Transmitted: May 8, 2024

For the full report click [here](#)

The Whistleblower Protection Enhancement Act requires federal agencies that have or use nondisclosure policies, forms, or agreements ensure that said policies, forms, or agreements include an explicit statement (“anti-gag provision”) notifying the signatory employees that they retain their rights to report wrongdoing to Congress, the Inspector General, or the Office of Special Counsel. The CPSC was not compliant with the anti-gag provision of the Whistleblower Protection Enhancement Act in two recent non-disclosure agreements. The CPSC has acted to remedy this non-compliance going forward.





## **OIG Coordination**

### **Council of the Inspectors General on Integrity and Efficiency**

The Inspector General maintains active membership in CIGIE and its associated subcommittees. CIGIE identifies, reviews, and discusses issues that are of interest to the entire OIG community. The Inspector General serves on the Audit, Legislation, and Inspection and Evaluation Committees, the Audit Peer Review Subcommittee, and as an adjunct instructor for the CIGIE Training Institute. The Inspector General regularly attends meetings held by CIGIE and their joint meetings with the Government Accountability Office.

The OIG staff attended seminars and training sessions sponsored or approved by CIGIE. OIG staff are also active participants in a variety of CIGIE subgroups including, but not limited to, the Deputy Inspectors General group, the management and planning group, and groups covering topics such as investigations, information technology, FISMA, PIIA, and financial statement audits.

### **Council of Counsels to the Inspectors General**

The Counsel to the Inspector General is a member of the Council of Counsels to the Inspectors General (CCIG). The CCIG considers legal issues of interest to the Offices of Inspectors General. During the review period, the Counsel met with peers to discuss items of mutual interest to all OIGs. The Counsel also participates in the CCIG National Defense Authorization Act Working Group (including the Definitions subgroup), CCIG Investigative Counsel working group, Freedom of Information Act working group, and Small OIG Counsel group.



## Peer Reviews

The OIG has previously completed work under both *Generally Accepted Government Auditing Standards* (GAGAS) and CIGIE QSIE. Each standard-setting body requires the organization to obtain an external review of its system of quality control every three years and make the results publicly available. The OIG continues to perform work utilizing GAGAS but now only utilizes CIGIE QSIE for work that is contracted out.

### GAGAS Peer Reviews

On March 31, 2023, the Ability One 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, 2022, had been "suitably designed and complied with to provide the CPSC OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects with Government Auditing Standards and applicable legal and regulatory requirements." Audit organizations can receive a rating of pass, pass with deficiencies, or fail. We received an External Peer Review rating of pass. This peer review is on our website [here](#).

On December 15, 2022, the CPSC OIG completed a peer review of the Library of Congress' Office of Inspector General. They received an External Peer Review rating of pass.

### CIGIE QSIE Peer Reviews

On March 10, 2023, the Architect of the Capitol Office of Inspector General issued a report of its External Peer Review of our Inspection and Evaluation organization and opined "that the CPSC OIG's policies and procedures generally complied and were consistent with Standard 7 - Quality Control of the QSIE standards addressed in the external peer review." Inspection and Evaluation Organizations can receive a rating of "generally complied" or "did not generally comply" with QSIE standards. We received a rating of "generally complied" with applicable standards. This peer review is available on our website [here](#).

On July 14, 2023, the CPSC OIG completed a peer review of the Office of the Special Inspector General for the Troubled Asset Relief Program's Inspection and Evaluation organization. They received a peer review rating of "generally complied" with applicable standards.



## 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.	8-9
Section 5(a)(1)	Significant problems, abuses, and deficiencies relating to the administration of programs and operations of the establishment and associated reports and recommendations for corrective action made by the OIG.	5, 16-23
Section 5(a)(2)	An identification of each recommendation made before the reporting period, for which corrective action has not been completed, and identification of cost savings associated with the recommendation.	16-23
Section 5(a)(3)	A summary of significant investigations closed during this reporting period.	6
Section 5(a)(4)	An identification of the total number of convictions during the reporting period resulting from investigations.	6
Section 5(a)(5)	Information regarding each audit, inspection, or evaluation, total dollar value of questioned costs and funds put to better use during this reporting period.	5
Section 5(a)(6)	Information regarding any management decision made during the reporting period with respect to any audit, inspection, or evaluation issued during a previous reporting period.	NA
Section 5(a)(7)	Information under section 804(b) of Federal Financial Management Improvement Act of 1996.	NA
Section 5(a)(8)	Results of peer review.	11
Section 5(a)(9)	Outstanding recommendations from any peer review conducted by another OIG.	NA
Section 5(a)(10)	Any peer reviews performed of another OIG.	11
Section 5(a)(11)	Statistical table showing total number of investigative reports, referrals, and results of referrals.	6
Section 5(a)(12)	Metrics used to develop data for tables in section 5(a)(11).	6
Section 5(a)(13)	Report on each investigation involving a senior government official where allegations of misconduct are substantiated.	6
Section 5(a)(14)	Detailed description of whistleblower retaliation.	NA
Section 5(a)(15)	Detailed description of attempts to interfere with OIG independence.	7
Section 5(a)(16)	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: 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	
CCIG	Council of Counsels to the Inspectors General
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CPSA	Consumer Product Safety Act
CPSC or Commission	U. S. Consumer Product Safety Commission
CPSIA	Consumer Product Safety Improvement Act of 2008
FISMA	Federal Information Security Modernization Act
FMFIA	Federal Managers' Financial Integrity Act
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
IG Act	The Inspector General Act of 1978, as amended
Kearney	Kearney & Company
KPMG	KPMG, LLP
M	Memorandum
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIIA	Payment Integrity Information Act
QSIE	Quality Standards for Inspection and Evaluation
Williams Adley	Williams, Adley & Company-DC, LLP





## APPENDIX C: STATUS OF RECOMMENDATIONS

---

During the most recent reporting period the agency submitted 76 requests for closure. During the same period, we found that the agency had successfully closed 32 recommendations. One closure related to the PIIA audit which, because of the semiannual reporting cycle, does not yet appear on the chart which follows. Due to a staffing shortage, we were unable to complete our review of 10 of the requests for closure. To offset both our staffing shortfall and our current lack of an IT auditor, we retained the services of a contractor to review requests for closure of IT-related recommendations. The contractor will complete its review of additional requests for closure early in the next semiannual period.

The 76 recommendations proposed for closure were a marked improvement over the 21 proposed for closure during the preceding semiannual period. The agency has reported that they are placing renewed emphasis on implementing recommendations and it appears that this effort is bearing fruit.

### **The Good Accounting Obligation in Government Act**

The Good Accounting Obligation in Government Act, enacted in 2019, requires agencies to provide, along with their annual budget request, a report that includes a list of unimplemented recommendations, an explanation of the reasons why no final action has been taken regarding the unimplemented recommendations, and a timeline for the implementation of unimplemented recommendations.

The Inspector General notes that the agency's Good Accounting Obligation in Government Act report dated January 30, 2024, does not include the required explanation of the reasons why no final action was taken regarding unimplemented recommendations.



The table below provides a summary of reports with open recommendations made before the current semiannual period and shows progress made during the last six months.

Summary of Recommendation Implementation Progress							
Report Short Title	Report Date	Total Recommendations	Closed Prior to April 1, 2024	Open as of April 1, 2024	Closed during the period	Open as of September 30, 2024	Total Days Past Due as of September 30, 2024
RMS	6/5/2012	8	3	5	0	5	4320
CYBER	8/4/2016	5	0	5	1	4	2799
TELEWORK	9/29/2017	9	8	1	0	1	2378
OEP	6/7/2018	12	6	6	0	6	2127
PROPERTY	5/31/2019	25	10	15	0	15	1769
PENTEST	6/11/2019	40	33	7	1	6	1758
BREACH	9/25/2020	40	19	21	14	7	1286
FDS	4/16/2021	4	0	4	0	4	1083
PD*	4/29/2021	13	1	12	0	12	1070
FMFIA	5/12/2021	7	0	7	0	7	1057
FISMA 21	10/29/2021	47	11	36	7	29	887
NIST CSF	1/18/2022	5	0	5	0	5	806
FISMA 22**	7/22/2022	4	0	4	0	4	621
PENTEST 22	12/13/2022	14	9	5	1	4	477
HR ASSESSMENT*	3/30/2023	41	0	41	1	40	370
FISMA 23**	7/28/2023	14	0	14	5	9	250
Cloud	1/31/2024	6	0	6	1	5	63
FSA 23	2/2/2024	16	0	16	0	16	61
		<b>310</b>	<b>100</b>	<b>210</b>	<b>31</b>	<b>179</b>	

\*One recommendation from the PD audit and six recommendations from the HR Assessment are no longer monitored due to agency non-concurrence.

\*\*FISMA 22 has a total of 24 recommendations, 20 of which were carried over from prior years. FISMA 23 has a total of 44 recommendations, 30 of which are carried over from prior years.



## **Previously Issued Reports with Open Recommendations**

Please see the links below for open recommendations for each report.

### **Consumer Product Safety Risk Management System Information Security Review Report (RMS)**

Transmitted: June 5, 2012

For the full report and list of open recommendations click [here](#)

The objective of this review was to evaluate the application of the Risk Management Framework to the Consumer Product Safety Risk Management System. CPSIA requires the CPSC to implement a publicly accessible and searchable database of consumer product incident reports. The period of the review was December 2010 through February 2011. 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 this database.

### **Cybersecurity Information Sharing Act of 2015 (CYBER)**

Transmitted: August 4, 2016

For the full report and list of open recommendations click [here](#)

The objective of this review was to determine whether the CPSC had established the policies, procedures, and practices required by the Cybersecurity Act of 2015 for agency systems that contain Personally Identifiable Information. During this review, we also considered whether standards for logical access were appropriate. The OIG completed this work in accordance with CIGIE QSIE. We found the CPSC had not achieved a number of the requirements set forth in the Cybersecurity Act of 2015 or developed appropriate logical access policies and procedures.

### **Audit of the Telework Program for Fiscal Year 2016 (TELEWORK)**

Transmitted: September 29, 2017

For the full report and list of open recommendations click [here](#)

The objectives of this audit were to determine if the CPSC had an effective program in place to capitalize on the benefits of telework, established adequate internal controls over telework, and administered the telework program in accordance with federal laws, regulations, guidance, and agency policy. The audit was performed in accordance with GAGAS. Overall, we found that the agency had a policy; however, it was not entirely effective and did not fully comply with federal laws, regulations, and agency policy.



### **Audit of the Occupant Emergency Program for Fiscal Year 2017 (OEP)**

Transmitted: June 7, 2018

For the full report and list of open recommendations click [here](#)

The OIG audited the CPSC's Occupant Emergency Program in place for FY 2017. The purpose of an Occupant Emergency Program is to reduce the threat of harm to personnel, property, and other assets within a federal facility in the event of an emergency. The objectives of this audit were to determine program effectiveness and compliance with the Occupant Emergency Program: *An Interagency Security Committee Guide* and other criteria. The audit was performed in accordance with GAGAS. Overall, we found that the CPSC's Occupant Emergency Program was not compliant with government-wide guidance and was not operating effectively.

### **Review of Personal Property Management System and Practices for the Calendar Year 2017 (PROPERTY)**

Transmitted: May 31, 2019

For the full report and list of open recommendations click [here](#)

The OIG contracted with Kearney & Company (Kearney) to perform an assessment of the CPSC's control over personal property. The objective was to obtain an independent review of the controls over personal property items, from initial data entry through routine accounting control to disposal. The review was performed in accordance with CIGIE QSIE. Overall, Kearney found that the CPSC's Personal Property Management System and practices were neither compliant with government-wide guidance nor operating effectively.

### **Report on the Penetration and Vulnerability Assessment of CPSC's Information Technology Systems (PENTEST)**

Transmitted: June 11, 2019

For the full report and list of open recommendations click [here](#)

The OIG contracted with Defense Point Security to perform a penetration and vulnerability assessment of the CPSC network. The objective of this penetration test was to assess the security of the CPSC's information technology infrastructure by safely attempting to exploit security vulnerabilities. The review was performed in accordance with CIGIE QSIE. Overall, Defense Point Security found that the CPSC had not designed its information technology infrastructure to be compliant with government-wide guidance and that its information technology infrastructure was not adequately secure.





## **Report of Investigation Regarding the 2019 Clearinghouse Data Breach (BREACH)**

Transmitted: September 25, 2020

For the full report and list of open recommendations click [here](#)

The OIG was asked to investigate a data breach involving the CPSC's Clearinghouse. We determined that the scope of the data breach exceeded the CPSC's estimate in terms of both duration and quantity. The data breach was caused by a combination of mismanagement and incompetence. CPSC employees caused the data breach by inappropriately releasing confidential information. The CPSC's reliance on Clearinghouse management to assess the scope of the breach led to a minimization of the range of the data breach and adversely affected the CPSC's efforts to respond to the data breach. We found a near total lack of: supervisory review, documented policies and procedures, and training for non-supervisory and first level supervisory employees carrying out Clearinghouse duties. These problems were compounded by management's lack of integrity regarding the dearth of properly designed and implemented internal controls. For years, agency management signed statements of assurance affirming that there were effective internal controls in place over the Clearinghouse, despite knowing this was not true.

## **Evaluation of the CPSC's Implementation of the Federal Data Strategy (FDS)**

Transmitted: April 16, 2021

For the full report and list of open recommendations click [here](#)

The OIG contracted with Williams Adley to perform a review of the CPSC's implementation of the Federal Data Strategy. The objective of this review was to obtain an independent evaluation of the CPSC's implementation of the OMB M-19-18, *Federal Data Strategy - A Framework for Consistency*, and associated OMB-issued action plans. The review was performed in accordance with CIGIE QSIE. Williams Adley found that the CPSC completed the required agency actions described in the most recent action plan published by OMB and provided recommendations to aid the CPSC in maturing its data management program.

## **Audit of the CPSC's Position Designation and Suitability Program (PD)**

Transmitted: April 29, 2021

For the full report and list of open recommendations click [here](#)

The OIG audited the CPSC position designation process. Each covered federal position is required to have a designation level (Tier 1 through Tier 5), depending on the sensitivity and risk



level of the position. The objectives of this audit were to determine whether all positions in the CPSC were appropriately designated and whether all CPSC employees and contractors have the appropriate background investigation completed. The audit was performed in accordance with GAGAS. The audit identified \$49,631 in questioned costs.

### **Audit of the CPSC's Implementation of FMFIA for FYs 2018 and 2019 (FMFIA)**

Transmitted: May 12, 2021

For the full report and list of open recommendations click [here](#)

The OIG contracted with Kearney to perform an audit of the CPSC's compliance in FYs 2018 and 2019 with the Federal Managers' Financial Integrity Act (FMFIA). Kearney was also charged with evaluating the effectiveness of the CPSC's processes to assess internal control over program operations, as reported in the Chairman's Management Assurance Statement in the Agency Financial Report. The review was performed in accordance with GAGAS. Kearney determined that the CPSC did not comply with the FMFIA in FYs 2018 and 2019. Specifically, a misalignment existed between how the CPSC identified programmatic or operational activities, how it measured the performance of these activities, and how it reported these activities. Additionally, although the CPSC implemented metrics to monitor the performance of its strategic goals and objectives, it did not establish and implement a formal internal controls program over its operations as required by the Government Accountability Office's, *Standards for Internal Control in the Federal Government*, and OMB Circular A-123, *Management's Responsibility for Internal Control*.

### **Evaluation of the CPSC's FISMA Implementation for FY 2021 (FISMA 21)**

Transmitted: October 29, 2021

For the full report and list of open recommendations click [here](#)

The OIG contracted with Williams Adley to review the CPSC's compliance with the reporting requirements of FISMA in FY 2021. The objective of this review was to determine the effectiveness of the CPSC's information security program in accordance with the FY 2021 FISMA reporting requirements issued by the Department of Homeland Security and OMB M-21-02, *FY 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*. The review was performed in accordance with CIGIE QSIE. Williams Adley found that the CPSC was not compliant with all of FISMA's requirements. However, the CPSC was making progress in implementing many FISMA requirements.



### **NIST Cybersecurity Framework (CSF)**

Transmitted: January 18, 2022

For the full report and list of open recommendations click [here](#)

The OIG contracted with Williams Adley to perform a review of the CPSC's implementation of the *National Institute of Standards and Technology Cybersecurity Framework* (NIST CSF). The objective of this requirement was to obtain an independent evaluation of the CPSC's implementation of the NIST CSF. The review was performed in accordance with CIGIE QSIE. Williams Adley found that the CPSC had developed a high-level action plan for the NIST CSF in 2017, however, the CPSC had not implemented that plan.

### **Evaluation of the CPSC's FISMA Implementation for FY 2022 (FISMA 22)**

Transmitted: July 22, 2022

For the full report and list of open recommendations click [here](#)

The OIG contracted with Williams Adley to review the CPSC's compliance with the reporting requirements of FISMA for FY 2022. The objective of this review was to determine the effectiveness of the CPSC's information security program in accordance with the FY 2022 FISMA reporting requirements, issued by the Department of Homeland Security and OMB M-22-05, *Fiscal Year 2021-2022 Guidance of Federal Information Security and Privacy Management Requirements*. As a result of changes in OMB requirements, this year was the first under the new continuous monitoring model. Williams Adley reviewed a subset of 20 "core" and 20 "non-core" metrics that were in scope for FY 2022. The review was performed in accordance with CIGIE QSIE. Williams Adley found that the CPSC was not compliant with all of FISMA's requirements. However, the CPSC was making progress in implementing many FISMA requirements.

### **Penetration Test 2022 (PENTEST 22)**

Transmitted: December 13, 2022

For the full report and list of open recommendations click [here](#)

The OIG contracted with Williams Adley to perform a penetration and vulnerability assessment of the CPSC network. Williams Adley subcontracted the assessment to Cerberus Sentinel. The objective of this penetration test was to assess the security of the CPSC's information technology infrastructure by safely attempting to exploit security vulnerabilities. The review was performed



in accordance with CIGIE QSIE. Overall, Cerberus Sentinel found that the CPSC had not designed its information technology infrastructure to be compliant with government-wide guidance and that its information technology infrastructure was not adequately secure.

### **Human Resources Assessment (HR ASSESSMENT)**

Transmitted: March 30, 2023

For the full report and list of open recommendations click [here](#)

The OIG contracted with AE Strategies to evaluate the CPSC's human resources function's ability to provide adequate support to the CPSC as the agency experiences a period of rapid growth. AE Strategies evaluated the human resources function using the Human Capital Framework evaluation model. This review was performed using Office of Personnel Management assessment tools to address strategic planning, talent management, performance management, and human resource performance evaluation topics.

AE Strategies found that the CPSC's human capital program did not align with federal regulations and lacked overall accountability. If not corrected, these shortcomings may prevent the CPSC from achieving its mission. Many of the findings and recommendations found in this assessment were over two decades old and were first identified in Office of Personnel Management evaluations in 1998 and 2008. These recommendations were never resolved, including a finding that the CPSC had not established a system of accountability to ensure that its human capital program is managed effectively and efficiently.

### **Evaluation of the CPSC's FISMA implementation for FY 2023 (FISMA 23)**

Transmitted: July 28, 2023

For the full report and list of open recommendations click [here](#)

The OIG contracted with Williams Adley to review the CPSC's compliance with the reporting requirements of FISMA for FY 2023. The objective of this review was to determine the effectiveness of the CPSC's information security program in accordance with the FY 2023 FISMA reporting requirements, issued by the Department of Homeland Security and OMB M-23-03, *Fiscal Year 2023 Guidance of Federal Information Security and Privacy Management Requirements*. As a result of recent changes in OMB requirements, this year was the second year under the new continuous monitoring model. Therefore, Williams Adley reviewed only the subset of 20 "core" and 20 "non-core" metrics that were in scope for FY 2023. The review was





performed in accordance with CIGIE QSIE.

Williams Adley found that the CPSC was not compliant with all of FISMA's requirements. However, the CPSC was making progress in implementing many FISMA requirements.

### **Evaluation of the CPSC's Management of Cloud Computing, Shared Services, & Third-Party Systems (CLOUD)**

Transmitted: January 31, 2024

For the full report and list of open recommendations click [here](#)

The OIG contracted with Williams Adley to obtain an independent evaluation of the CPSC's Cloud Computing, Third-Party, and Shared Service management from a legal, internal control, and contractual perspective. The evaluation was performed in accordance with the CIGIE QSIE.

Williams Adley found that the CPSC utilizes cloud computing, shared services, and third-party systems to support its mission and operations. However, Williams Adley identified areas for improvement. As a result of the evaluation, Williams Adley made six recommendations to improve the CPSC's management of its cloud computing, third-party, and shared services providers.

### **Audit of the Consumer Product Safety Commission's Fiscal Year 2023 Financial Statements (FSA 23)**

Transmitted: February 2, 2024

For the full report and list of open recommendations click [here](#)

The OIG contracted with KPMG, an independent public accounting firm, to perform an independent audit of the CPSC's financial statements according to all current standards for the period ending September 30, 2023. The objective of this audit was to determine whether the CPSC's financial statements present fairly the financial position of the agency and were compliant with relevant laws and regulations. The CPSC was required to submit audited financial statements in accordance with the Accountability of Tax Dollars Act of 2002, which retroactively implements the Chief Financial Officers Act of 1990 for smaller agencies, including the CPSC. This audit was performed in accordance with GAGAS.



KPMG issued a qualified opinion of the financial statements due to the agency A) inappropriately calculating the accumulated depreciation and depreciation expense related to its Property, Plant, and Equipment; and B) being unable to recalculate said accumulated depreciation and depreciation expense in a timely manner. Other than this matter, KPMG determined the financial statements present fairly the financial position of the agency and were compliant with relevant laws and regulations. In total, KPMG identified three material weaknesses and one significant deficiency of internal controls over financial reporting and made 16 recommendations to improve the CPSC's internal control system.





For more information on this report please contact us at [CPSC-OIG@cpsc.gov](mailto:CPSC-OIG@cpsc.gov)

To report fraud, waste, or abuse, mismanagement, or wrongdoing at the CPSC go to  
[OIG.CPSC.GOV](http://OIG.CPSC.GOV) or call (301) 504-7906

Office of Inspector General, CPSC, 4330 East-West Hwy., Suite 702, Bethesda, MD 20814