



# Office of Inspector General

U.S. Consumer Product Safety Commission

## Semiannual Report to Congress October 1, 2020 to March 31, 2021

April 30, 2021

Report 21-O-05

## **Vision Statement**

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

## **Statement of Principles**

We will:

Work with the Commission and the Congress to improve program management.

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

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

Be innovative, question existing procedures, and suggest improvements.

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

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

Work together to address government-wide issues.



April 30, 2021

TO: Robert S. Adler, Acting Chairman  
Elliot F. Kaye, Commissioner  
Dana Baiocco, Commissioner  
Peter A. Feldman, Commissioner

FROM: Christopher W. Dentel, Inspector General *Christopher W. Dentel*

SUBJECT: Transmittal of the Semiannual Report

I am pleased to present this Semiannual Report summarizing the activities of our office for the period October 1, 2020, through March 31, 2021. The U.S. Consumer Product Safety Commission (CPSC or Commission) Office of Inspector General (OIG) remains committed to promoting the economy, efficiency, and effectiveness of the CPSC's programs and operations. Our audits, special projects, and investigative work reflect our commitment to keep the Congress, the Commission, and the American people 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.

Over the past five reporting periods, the closure rate of agreed to recommendations has shown a steady decline. While the agency has made progress closing recommendations previously, during this most recent reporting period, management closed only five recommendations.

In addition to our work with the CPSC, the OIG continues to be involved with the Council of the Inspectors General on Integrity and Efficiency and the Council of Counsels to the Inspectors General on issues of interest to the entire OIG community. 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.

## **Contents**

Background .....	1
U.S. Consumer Product Safety Commission .....	1
Office of Inspector General .....	1
Audit Program .....	3
Completed Reports .....	3
Ongoing Projects .....	5
Previously Issued Reports with Open Recommendations .....	7
Reportable Investigations .....	13
Other Activities .....	15
Legislation and Regulatory Review .....	15
OIG Coordination.....	16
Appendix A: Cross-Reference to Reporting Requirements of the IG Act .....	17
Appendix B: Peer Reviews.....	18
Appendix C: Statement Regarding Plain Writing .....	20
Appendix D: Status of Recommendations.....	21

## **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 Federal Hazardous Substances Act, the Flammable Fabrics Act, the Poison Prevention Packaging Act, the Refrigerator Safety Act, the Virginia Graeme Baker Pool and Spa Safety Act, the Child Safety Protection Act, the Labeling of Hazardous Art Materials Act, the Children’s Gasoline Burn Prevention Act, the Drywall Safety Act of 2012, and the Child Nicotine Poisoning Prevention Act.

The CPSC’s mission is “Keeping Consumers Safe.” Congress granted the CPSC broad authority to issue and enforce standards prescribing performance requirements, warnings, or instructions regarding the use of consumer products under the CPSA and CPSIA, as well as numerous other laws.

By statute, the CPSC is headed by five Commissioners appointed by the president with the advice and consent of the Senate. The Chairman of the CPSC is designated by the president as the principal executive officer of the Commission.

The CPSC’s headquarters is located in Bethesda, Maryland. The CPSC also operates the National Product Testing and Evaluation Center in nearby Rockville, Maryland and has field personnel throughout the country.

### **Office of Inspector General**

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

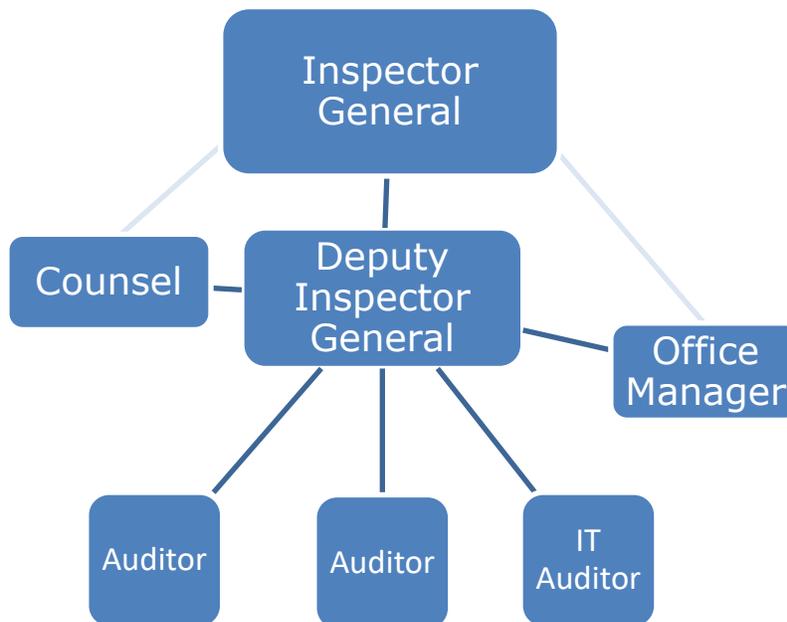
The IG Act was amended by the Inspector General Empowerment Act of 2016. The Inspector General Empowerment Act safeguards OIG access to agency information and mandates additional reporting to increase transparency in government operations.

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

- conduct and supervise audits and investigations of the CPSC’s programs and operations
- provide leadership, coordination, and recommend policies for activities designed to promote economy, efficiency, and effectiveness in the administration of the CPSC’s programs and operations
- prevent and detect fraud, waste, and abuse of the CPSC’s programs and operations
- keep the Commissioners and the Congress fully and currently informed about problems and deficiencies relating to the administration of the CPSC’s programs and operations and the need for progress or corrective action

We strive to offer 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.

### **Office of Inspector General Organizational Chart**



## **Audit Program**

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

### **Completed Reports**

#### **EVALUATION OF CPSC'S FISMA IMPLEMENTATION FOR FY 2020**

Transmitted: November 3, 2020

For the full report 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 Federal Information Security Modernization Act (FISMA) for fiscal year (FY) 2020. The objective of this review was to determine the effectiveness of the CPSC's information security program in accordance with the FY 2020 FISMA reporting requirements, issued by the Department of Homeland Security and Office of Management and Budget Memorandum (OMB M)-20-04, *Fiscal Year 2019-2020 Guidance of Federal Information Security and Privacy Management Requirements*. The review was performed in accordance with Council of the Inspectors General for Integrity and Efficiency (CIGIE) Quality Standards for Inspection and Evaluation (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 47 recommendations to improve the CPSC's information security posture. CPSC's progress in resolving these recommendations will be evaluated as part of the FY 2021 FISMA evaluation.

#### **REVIEW OF THE CPSC'S NEISS PROGRAM**

Transmitted: November 9, 2020

For the full report click [here](#)

The OIG contracted with Kearney & Company (Kearney) to review the CPSC's National Electronic Injury Surveillance System (NEISS) program. The NEISS program creates an average of 350,000 records per year. The data contained in these records can be used to raise consumer awareness of emerging product safety hazards, to support detailed studies that provide data on the number and types of injuries associated with specific products, and to inform standards development. The review was conducted in accordance with CIGIE QSIE. Kearney determined that the NEISS program did not have an adequate data governance program in

place to ensure data quality. Additionally, the CPSC could not provide documentation to establish that a legal opinion was obtained before the CPSC expanded the NEISS program to include data on injuries outside of the CPSC's jurisdiction. Finally, the CPSC could not provide sufficient documentation to support estimated costs charged to other federal agencies as required by the Economy Act when using Interagency Agreements. This review makes 12 recommendations to improve NEISS data governance and support the methodology to determine costs charged to other agencies and all 12 remain open.

#### AUDIT OF THE CPSC'S FY 2020 FINANCIAL STATEMENTS

Transmitted: November 16, 2020

For the full report click [here](#)

The OIG contracted with CliftonLarsonAllen, LLP (CLA), an independent public accounting firm, to perform an independent audit of the CPSC's financial statements according to all current standards for the period ended September 30, 2020. The objective of this audit was to determine whether the CPSC's financial statements presented fairly the financial position of the agency and are compliant with relevant laws and regulations. The CPSC is required to submit audited financial statements in accordance with the Accountability of Tax Dollars Act of 2002, which retroactively implements the Chief Financial Officers Act of 1990 for smaller agencies, including the CPSC. This audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS). CLA identified a significant deficiency in internal control regarding the monitoring and tracking of the amortization of leasehold improvements and automated data processing software, and a reportable violation of fiscal law. This audit makes two recommendations to improve controls over asset accounting. The CPSC's progress in resolving these recommendations will be evaluated as part of the FY 2021 Financial Statement Audit.

#### THE OFFICE OF INSPECTOR GENERAL'S SURVEY ON THE TRANSITION TO MANDATORY FULLTIME TELEWORK

Transmitted: February 9, 2021

For the full report click [here](#)

After transitioning to mandatory fulltime telework (MFT) on March 16, 2020, due to the COVID-19 pandemic, the OIG decided it was important to survey CPSC staff about concerns and positive experiences during MFT related to: the amount and types of communication from management, support from the information technology Help Desk, videoconferencing options, productivity and supervision during MFT, and the future of telework. This was a special project outside the OIG work plan and was not performed in accordance with GAGAS. Overall, the OIG found that employees have a positive view of MFT and the agency's

management of the transition. There has been a shift in attitudes in favor of the CPSC providing more telework opportunities in the future. This appears to have been driven by employees and supervisors gaining experience with telework and seeing few, if any, drawbacks. This report made no recommendations.

#### AUDIT OF THE OFFICE OF COMMUNICATIONS MANAGEMENT'S STRATEGIC GOALS

Transmitted: February 19, 2021

For the full report click [here](#)

The OIG audited the CPSC's Office of Communications Management's (OCM) strategic goals for FYs 2018 and 2019. The objectives of the audit were to assess OCM's methodology for developing key performance measures, implementing their strategic initiatives, and reporting on the results of the effectiveness of those strategic initiatives. Additionally, we assessed OCM's internal controls over the dissemination of consumer product safety information and collaboration with stakeholders. The audit was conducted in accordance with GAGAS. The OIG determined that while OCM met or exceeded their targeted number of communications to the public, we identified several areas where OCM's internal controls over its performance reporting could be improved, particularly in the area of tracking communication quality and effectiveness. The OIG made 11 recommendations to improve data quality and reliability and all 11 remain open.

### **Ongoing Projects**

#### EVALUATION OF THE CPSC'S IMPLEMENTATION OF THE FEDERAL DATA STRATEGY 2020 ACTION PLAN

The OIG contracted with Williams Adley to perform a review of the CPSC's implementation of the Federal Data Strategy. The objective of this requirement is 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 is being performed in accordance with CIGIE QSIE.

#### REVIEW OF THE CPSC'S EQUAL EMPLOYMENT OPPORTUNITY PROGRAM

The OIG contracted with GKA, P.C., to perform an independent review of the CPSC's equal employment opportunity (EEO) program. The objectives of this review will be to determine whether the EEO program is in compliance with all statutory requirements and to assess the accuracy, completeness, and reliability of

the information reported. Federal agencies are required to annually report EEO activity to the U.S. Equal Employment Opportunity Commission. This review is being performed in accordance with CIGIE QSIE.

#### AUDIT OF THE CPSC'S IMPLEMENTATION OF FMFIA FOR FY 2018 AND 2019

The OIG contracted with Kearney to perform an audit of the CPSC's compliance with the Federal Managers' Financial Integrity Act (FMFIA) in FYs 2018 and 2019. 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, as published in the Agency Financial Report. The review is being performed in accordance with GAGAS.

#### AUDIT OF THE CPSC'S POSITION DESIGNATION PROCESS

The OIG is auditing 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 are to determine whether all positions in the CPSC are appropriately designated and whether all CPSC employees and contractors have the appropriate background investigation completed. The audit is being performed in accordance with GAGAS.

#### REVIEW OF THE CPSC'S COMPLIANCE WITH THE PAYMENT INTEGRITY INFORMATION ACT FOR FISCAL YEAR 2020

The OIG contracted with Kearney to perform a review of the CPSC's compliance with the reporting requirements contained in the Payment Integrity Information Act (PIIA), for transactions in FY 2020. The review focuses on the CPSC's compliance with the six elements identified as criteria in the OMB guidance, as well as overall program internal controls. The review is being performed in accordance with CIGIE QSIE.

#### THE OFFICE OF INSPECTOR GENERAL'S SURVEY ON EMPLOYEE RETURN TO REGULAR WORK LOCATIONS

This survey was undertaken to understand employee concerns about returning to their regular work location. The goals of the survey are to identify employee concerns to help with the transition away from fulltime mandatory telework as the pandemic eases. The survey also covered employee views on continued communication from management about returning to work and views about

preferred work schedules and locations in the future. This is a special project, outside the OIG work plan, and is not performed in accordance with GAGAS.

## AUDIT OF THE CPSC'S FY 2021 FINANCIAL STATEMENTS

The OIG contracted with CLA to perform an independent audit of the CPSC's financial statements according to all current standards, for the period ending September 30, 2021. The objective of this audit is to determine whether the CPSC's financial statements present fairly the financial position of the agency and are compliant with relevant laws and regulations. The CPSC is required to submit audited financial statements in accordance with the Accountability of Tax Dollars Act of 2002, which retroactively implements the Chief Financial Officers Act of 1990 for smaller agencies, including the CPSC. This audit is being performed in accordance with GAGAS.

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

Please see [Appendix D](#) for a consolidated list of open recommendations.

#### CONSUMER PRODUCT SAFETY RISK MANAGEMENT SYSTEM INFORMATION SECURITY REVIEW REPORT

Transmitted: June 5, 2012

For the full report click [here](#)

The objective of this review was to evaluate the application of the Risk Management Framework to the Consumer Product Safety Risk Management System (CPSRMS). 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. There were eight consolidated recommendations associated with this report and five remain open.

#### OPPORTUNITIES EXIST TO ENSURE CPSC EMPLOYEES ARE SATISFYING IN GOOD FAITH THEIR JUST FINANCIAL OBLIGATIONS

Transmitted: September 30, 2014

For the full report click [here](#)

The objective was to determine whether the CPSC had established adequate internal controls over employee wage garnishments and appropriate tax withholdings. The OIG conducted a review of the CPSC's efforts to ensure its

employees were satisfying their financial obligations in good faith, especially those related to federal, state, or local taxes. We also assessed the CPSC's compliance with identified applicable laws, regulations, and court ordered judgments. This review was conducted in accordance with CIGIE QSIE. We determined that the CPSC Office of Human Resources Management had not established proper oversight procedures over wage garnishments processed by their service provider, the Interior Business Center of the U.S. Department of the Interior. There were two consolidated recommendations associated with this report and both remain open.

#### AUDIT OF THE FREEDOM OF INFORMATION ACT PROGRAM

Transmitted: September 30, 2015

For the full report click [here](#)

The objective of this audit was to determine whether the CPSC had developed proper internal controls over its Freedom of Information Act (FOIA) program. This included assessing the adequacy of the policies and procedures to comply with the FOIA laws and regulations. We also examined fee assessments for FOIA requests processed between October 1, 2008, and September 30, 2013. The OIG conducted this audit under GAGAS. We found that although the CPSC had a functioning program, we identified several internal control weaknesses and noted that the program did not comply with certain policies and procedures mandated by the FOIA. There were 11 consolidated recommendations associated with this report and 7 remain open.

#### CYBERSECURITY INFORMATION SHARING ACT OF 2015 REVIEW REPORT

Transmitted: August 14, 2016

For the full report click [here](#)

The objective of this review was to determine whether the CPSC had established the policies, procedures, and practices required by the Cybersecurity Act 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. There were five consolidated recommendations associated with this report and all five remain open.

## REPORT ON THE PERFORMANCE AUDIT OF INTERNAL CONTROLS OVER CONTRACT MANAGEMENT AND ADMINISTRATION FOR FISCAL YEAR 2016

Transmitted: July 25, 2017

For the full report click [here](#)

The objectives of this audit were to ascertain whether the CPSC had established and implemented effective internal controls to guide its contract and acquisitions management process for its firm-fixed-price contracts and whether the contract monitoring process utilized by the CPSC adhered to applicable federal laws and regulations. The OIG contracted with Kearney to complete this audit in accordance with GAGAS. Overall, Kearney found that the CPSC did not have an effective internal control system over its contract administration program. They made 14 recommendations to improve CPSC contract management and 1 remains open.

## AUDIT OF THE TELEWORK PROGRAM FOR FISCAL YEAR 2016

Transmitted: September 29, 2017

For the full report click [here](#)

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

## AUDIT OF THE OCCUPANT EMERGENCY PROGRAM FOR FISCAL YEAR 2017

Transmitted: June 7, 2018

For the full report click [here](#)

The OIG audited the CPSC's Occupant Emergency Program (OEP) in place for FY 2017. The purpose of an OEP 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 Interagency Security Committee Guide and other criteria. The audit was performed in accordance with GAGAS. Overall, we found that the CPSC's OEP was not compliant with government-wide guidance and was not operating effectively. To improve the safety of CPSC employees and other assets we made 12 recommendations and 10 remain open.

## AUDIT OF THE CPSC'S DIRECTIVES SYSTEM

Transmitted: March 21, 2019

For the full report click [here](#)

The OIG conducted an audit of the CPSC's Directives System operating until March 31, 2018. The objectives of this audit were to determine whether the CPSC's policies and procedures for the Directives System complied with federal regulations and procedures and were effective in helping agency staff meet the CPSC's mission. This audit was performed in accordance with GAGAS. Overall, we found that the CPSC's Directives System was not fully compliant with government-wide requirements, its own policies, or fully effective in helping staff to meet the CPSC's mission. We made two recommendations to improve the Directives System and one remains open.

## REVIEW OF PERSONAL PROPERTY MANAGEMENT SYSTEM AND PRACTICES FOR THE CALENDAR YEAR 2017

Transmitted: May 31, 2019

For the full report click [here](#)

The OIG contracted with Kearney to perform an assessment of the CPSC's control over personal property. The objective of this review 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. To improve the CPSC's Property Management System and processes Kearney made 25 recommendations and 18 remain open.

## REPORT ON THE PENETRATION AND VULNERABILITY ASSESSMENT OF CPSC'S INFORMATION TECHNOLOGY SYSTEMS

Transmitted: June 11, 2019

For the full report click [here](#)

The OIG contracted with Defense Point Security (DPS) 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, DPS 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. To improve the CPSC's information technology infrastructure DPS made 40 recommendations and 15 remain open.

#### AUDIT OF THE CPSC'S GRANTS PROGRAM

Transmitted: September 25, 2020

For the full report click [here](#)

The OIG audited the CPSC's Pool Safety Grants Program (PSGP) for all grants awarded prior to September 30, 2018. The objectives of this audit were to assess agency compliance with the laws and regulations that govern the PSGP, the overall effectiveness of the PSGP, the adequacy of the PSGP's internal control environment, and management's monitoring and administration of the program. The audit was performed in accordance with GAGAS. The OIG determined that the PSGP was not effective; and the audit identified \$1,722,084 in questioned costs.<sup>1</sup> The OIG made 22 recommendations to improve the PSGP and all 22 remain open.

#### REPORT OF INVESTIGATION REGARDING THE 2019 CLEARINGHOUSE DATA BREACH

Transmitted: September 25, 2020

For the full report 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 scope 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 lack 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

---

<sup>1</sup> Questioned costs are those costs that are questioned by the CPSC OIG because of an alleged violation of a provision of a law, regulation, contract, grant, cooperative agreement, or other agreement or document governing the expenditure of funds; costs not supported by adequate documentation; or a finding that the expenditure of funds for the intended purpose is unnecessary or unreasonable.

Clearinghouse, despite knowing this was not true. The OIG made 40 recommendations and all remain open.

## 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. During the reporting period, the OIG did not conduct any investigations involving a senior government employee where allegations of misconduct were substantiated nor did the OIG receive any actionable allegations of whistleblower retaliation. The table below summarizes the disposition of complaints and investigative work performed from October 1, 2020 through March 31, 2021.

Investigation Status	Count
<b>Open as of October 1, 2020</b>	<b>3</b>
Opened during reporting period	53
Closed during reporting period	3
Transferred to other Departments/Agencies	47
Referred to Department of Justice for Criminal Prosecution	0
Referred for State/Local Criminal Prosecution	0
Total Indictments/Information from Prior Referrals	0
<b>Open as of March 31, 2021</b>	<b>6</b>

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

### Reportable Investigations

**21-16** Complaint alleged a senior official was endorsing a product. After an inquiry, the allegation was determined to be unfounded and the investigation was closed.

**21-24** Complaint alleged a politically appointed employee was improperly transferred to a career position. The allegation was determined to be unfounded and the investigation was closed.

**21-25** Complaint alleged a senior official had recorded agency personnel without their knowledge or consent; demonstrated bullying and abusive behavior; and improperly shared confidential agency information with outside parties. The allegation regarding bullying and abusive behavior was already being investigated by the agency and was not accepted by the OIG for investigation. The other allegations are being investigated by OIG.

**21-44** Complaint regarding multiple issues related to returning to work at the agency: policy enforcement, Personal Protective Equipment availability, and mandatory fulltime telework eligibility. The complaint is not ripe for OIG investigation and has been referred to agency management.

## **Other Activities**

### **Legislation and Regulatory Review**

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

Anti-Deficiency Act  
Consumer Product Safety Act  
Consumer Product Safety Commission Regulations  
Consumer Product Safety Improvement Act of 2008  
Coronavirus Aid, Relief, and Economic Security Act (2020)  
Consolidated Appropriations Act, 2021  
Economy Act  
Ethics Regulations  
Executive Order on Combating Race and Sexual Stereotyping  
Families First Coronavirus Response Act  
Federal Acquisition Regulations  
Federal Sector Equal Employment Opportunity Complaint Processing Regulations  
Freedom of Information Act  
Hatch Act  
H.R. 1319 American Rescue Plan Act of 2021  
Inspector General Act of 1978, as amended  
Office of Management and Budget Circulars and Memoranda  
Public Disclosure of Information, 15 U.S.C. 2055  
Privacy Program  
Prohibited Personnel Practices  
Records Management Policies and Regulations  
Standards of Conduct for Government Employees  
Uniform Grant Guidance  
Virginia Graeme Baker Pool and Spa Safety Act  
Whistleblower Protection Enhancement Act

## **OIG Coordination**

### COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY

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

The OIG's staff attended seminars and training sessions sponsored or approved by CIGIE. 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. The Council considers legal issues of interest to the Offices of Inspectors General. During the review period, the Counsel met with peers to discuss items of mutual interest to all OIGs.

## Appendix A: Cross-Reference to Reporting Requirements of the IG Act

Citation	Reporting Requirements	Page(s)
Section 4(a)(2)	Review of legislation and regulations.	15
Section 5(a)(1)	Significant problems, abuses, and deficiencies.	3-5
Section 5(a)(2)	Recommendations with respect to significant problems, abuses, and deficiencies.	3-5
Section 5(a)(3)	Prior significant recommendations on which corrective action has not been completed.	7-12, 22-31
Section 5(a)(4)	Summary of matters referred to prosecutorial authorities and results.	NA
Section 5(a)(5)	Summary of each report made to head of agency when information was refused.	NA
Section 5(a)(6)	List of audit, inspection, and 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.	3-5
Section 5(a)(8)	Table showing the number of audit, inspection, and evaluation reports and dollar value of questioned costs for reports.	NA
Section 5(a)(9)	Table showing the 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.	7-12, 22-31
Section 5(a)(11)	Significant revised management decisions.	NA
Section 5(a)(12)	Significant management decisions with which the IG disagrees.	NA
Section 5(a)(13)	Information under section 804(b) of Federal Financial Management Improvement Act of 1996.	NA
Section 5(a)(14)	Results of peer review.	18-19
Section 5(a)(15)	Outstanding recommendations from any peer review conducted by another OIG.	NA
Section 5(a)(16)	Any peer reviews performed of another OIG.	18-19
Section 5(a)(17)	Statistical table showing total number of investigative reports, referrals, and results of referrals.	13
Section 5(a)(18)	Metrics used to develop data for table in section 5(a) (17).	13
Section 5(a)(19)	Report on each investigation involving a senior government official where allegations of misconduct are substantiated.	NA
Section 5(a)(20)	Detailed description of whistleblower retaliation.	NA
Section 5(a)(21)	Detailed description of attempt to interfere with OIG independence.	NA
Section 5(a)(22)	Detailed description of every inspection, evaluation, and audit closed and not publicly disclosed, and every investigation of senior government employee closed and not publicly disclosed.	NA

## **Appendix B: Peer Reviews**

The OIG has in the past completed work under both 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 through contractors.

### **GAGAS Peer Reviews**

On February 24, 2020, the Corporation for National and Community Service 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, 2019, 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." Audit organizations can receive a rating of pass, pass with deficiencies, or fail. We received an External Peer Review rating of pass. A copy of this peer review is on our [website](#).

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

### **Inspection and Evaluation (I&E) Peer Reviews**

On August 25, 2020, the Pension Benefit Guaranty Corporation Office of Inspector General issued a report of its Modified External Peer Review of our I&E organization and opined that our internal policies and procedures for the period ending June 30, 2020, are current and consistent with covered CIGIE QSIE standards. The seven required standards are Quality Control, Planning, Data Collection and Analysis, Evidence, Records Maintenance, Reporting, and Follow-up. The External Peer review was changed to a Modified Peer Review due to the impact and logistics of doing field work during a pandemic. For the full report click [here](#).

The CPSC OIG led a peer review team on December 16, 2019, to review the Office of Personnel Management Office of Inspector General I&E Organization. We opined

that their policies and procedures and work done for the period ending June 30, 2019, were current and consistent with the covered Blue Book standards.

## 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.

<b>Table of Abbreviations</b>	
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CLA	CliftonLarsonAllen, LLP
CPSA	Consumer Product Safety Act
CPSIA	Consumer Product Safety Improvement Act of 2008
CPSC and Commission	U.S. Consumer Product Safety Commission
CPSRMS	Consumer Product Safety Risk Management System
DPS	Defense Point Security
EEO	Office of Equal Employment Opportunity and Minority Enterprise
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
FMFIA	Federal Managers' Financial Integrity Act
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
I&E	Inspection and Evaluation
IG Act	The Inspector General Act of 1978, as amended
Kearney	Kearney & Company
M	Memorandum
MFT	Mandatory Fulltime Telework
NEISS	National Electronic Injury Surveillance System
OCM	Office of Communications Management
OEP	Occupant Emergency Program
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIIA	Payment Integrity Information Act
PSGP	Pool Safely Grants Program
QSIE	Quality Standards for Inspection and Evaluation
Williams Adley	Williams, Adley & Company-DC, LLP

## Appendix D: Status of Recommendations

During this most recent reporting period, management closed only five recommendations, all made relatively recently. In fact, in the past year, the CPSC has closed only one recommendation more than two years old. Over the past five reporting periods the closure rate has shown a steady decline. This chart provides a summary of reports with open recommendations as of the end of the 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 October 1, 2020	Open as of October 1, 2020	Closed during the period	Open as of March 31, 2020
RMS	6/5/2012	8	3	5	0	5
Debt	9/30/2014	2	0	2	0	2
FOIA	9/30/2015	11	4	7	0	7
Cybersecurity	8/14/2016	5	0	5	0	5
Contracts	7/25/2017	14	13	1	0	1
Telework	9/29/2017	9	4	5	0	5
OEP	6/7/2018	12	2	10	0	10
Directives	3/21/2019	2	1	1	0	1
Property	5/31/2019	25	3	22	4	18
Pentest	6/11/2019	40	24	16	1	15
Grants	9/25/2020	22	0	22	0	22
Breach	9/25/2020	40	0	40	0	40
		<b>190</b>	<b>54</b>	<b>136</b>	<b>5</b>	<b>131</b>

\*This chart does not include any recommendations from the Financial Statement Audit and FISMA. Those recommendations, if any, are addressed in the annual audit process.

The table below shows all open recommendations as of the end of the current semiannual period. As a reflection of the changing FISMA metrics, this table includes only the open recommendations from the most recent FISMA report prior to the current Semiannual Report period.

<i>Report Name and Date</i>	<i>Consolidated Recommendations</i>
<p data-bbox="224 411 683 541"><b>Consumer Product Safety Risk Management System Information Security Review Report (RMS)</b></p> <p data-bbox="224 573 402 604">June 5, 2012</p>	<p data-bbox="776 275 1354 373">RMS-1. Identify the participants of the CPSC Risk Executive Council and define specific tasks/milestones for implementing the proposed Risk Management Framework.</p> <p data-bbox="776 405 1354 504">RMS-2. Develop an Enterprise Architecture that includes a comprehensive IT security architecture using the CIO Council's guidance and incorporate this into the Security Control Documents.</p> <p data-bbox="776 535 1317 583">RMS-3. Fully document the implementation of the security controls.</p> <p data-bbox="776 615 1305 663">RMS-4. Update the CPSRMS SSP to be the single authoritative system security document.</p> <p data-bbox="776 695 1333 743">RMS-8. Define the specific Public Access controls in place/planned.</p>
<p data-bbox="224 814 691 945"><b>Opportunities Exist to Ensure CPSC Employees Are Satisfying in Good Faith Their Just Financial Obligations (Debt)</b></p> <p data-bbox="224 976 505 1008">September 30, 2014</p>	<p data-bbox="776 789 1338 919">Debt-1. Management develops and documents an internal process to effectively and actively monitor employee wage garnishments pursuant to a lawful court order and transferred from the Department of the Treasury's Treasury Offset Program.</p> <p data-bbox="776 951 1263 1045">Debt-2. Management develops a process to regularly, at least annually, review employee exemption and withholding status for reasonableness.</p>
<p data-bbox="224 1402 602 1501"><b>Audit of the Freedom of Information Act Program (FOIA)</b></p> <p data-bbox="224 1533 505 1564">September 30, 2015</p>	<p data-bbox="776 1073 1338 1255">FOIA-1. Revise and implement the CPSC FOIA Program directive and related appendices to ensure consistency with current legal requirements established by the FOIA to include document retention, training, fee assessment requirements, program monitoring, revenue reconciliation, timely updating of the public reading room.</p> <p data-bbox="776 1287 1338 1381">FOIA-3. Management develops SOP consistent with current FOIA legislation related to receipt, processing, and tracking of FOIA requests for IDI files.</p> <p data-bbox="776 1413 1317 1486">FOIA-5. Management develops a record retention schedule that complies with all current document retention requirements.</p> <p data-bbox="776 1518 1305 1612">FOIA-6. Management develops an effective FOIA monitoring system to measure timeliness of completion of all FOIA requests within statutory deadlines whether they should be assessed fees.</p> <p data-bbox="776 1644 1354 1738">FOIA-8. Develop and utilize guidance to determine subject(s) of frequent requests in the "reading room" and perform timely updates to reflect frequent requests.</p> <p data-bbox="776 1770 1338 1864">FOIA-10. Management develops standard operating procedures to provide guidance on compiling the annual report to the DOJ to include a documented supervisory review and sign-off.</p>

<i>Report Name and Date</i>	<i>Consolidated Recommendations</i>
	FOIA-11. Management documents a review of the data fields in FOIAXpress for accuracy, completeness, and timeliness.
<p><b>Cybersecurity Information Sharing Act of 2015 Review Report (Cyber)</b></p> <p>August 14, 2016</p>	<p>Cyber-1. Management updates, develops, and publishes general access control and logical access control policies and procedures for all systems that permit access to PII.</p> <p>Cyber-2. Provide training or document training completion by individual system owners on establishing, implementing, and maintaining logical access policies and procedures for systems that contain PII.</p> <p>Cyber-3. The General Access Control Policy and attendant procedures should be updated to include the elements outlined in the report.</p> <p>Cyber-4. Develop, document, and maintain a software inventory including license management policies and procedures.</p> <p>Cyber-5. Comply with and enforce HSPD-12 multifactor authentication supported by the Personal Identity Verification Card.</p>
<p><b>Report on the Performance Audit of Internal Controls over Contract Management and Administration for Fiscal Year 2016 (Contracts)</b></p> <p>July 25, 2017</p>	<p>Contracts-8. Obtain an attestation or audit of PRISM general and application controls routinely, preferably annually, and implement the resulting recommendations.</p>
<p><b>Audit of the Telework Program for Fiscal Year 2016 (Telework)</b></p> <p>September 29, 2017</p>	<p>Telework-1. Develop and implement a telework policy that is compliant with current federal laws, regulations, and OPM best practices where appropriate.</p> <p>Telework-2. Align agency practice and telework policy regarding employee participation and position eligibility.</p> <p>Telework-3. Document all decisions made with regard to position eligibility, individual participation including policy exceptions, participation limits, and termination of telework agreements.</p> <p>Telework-4. Design and implement a process to ensure that telework files are complete and regularly reviewed, at least biennially.</p> <p>Telework-5. Implement a process to validate telework information reported to outside parties and used for internal decision-making to internal source data on a routine basis.</p>

<i>Report Name and Date</i>	<i>Consolidated Recommendations</i>
<p><b>Audit of the Occupant Emergency Program for Fiscal Year 2017 (OEP)</b></p> <p>June 7, 2018</p>	<p>OEP-1. Clearly define all the roles to be used in the agency's OEP.</p> <p>OEP-3. Develop and implement an effective communication strategy to include ongoing awareness and general information for all facility occupants about the OEP and expectations.</p> <p>OEP-4. Develop and implement policies employing multiple communication channels for notifying staff during drills and emergency situations.</p> <p>OEP-5. Develop and implement occupant accountability procedures to be practiced during drills and used during emergencies.</p> <p>OEP-6. Develop and implement an effective OEP team training program with drills and exercises to include all team members at least annually.</p> <p>OEP-7. Develop and implement a corrective action process that reviews the results of all drills, exercises, and actual emergencies and documents whether to update OEP guidance, including showing the updated guidance.</p> <p>OEP-8. Develop and implement procedures to address the needs of individuals requiring additional assistance. These procedures should include a process to routinely update the list of persons requiring assistance.</p> <p>OEP-9. Develop and implement procedures to maintain, retain, and update OEP program documents at least semiannually.</p> <p>OEP-10. Develop and implement an annual round-table discussion with OEP coordinators and teams.</p> <p>OEP-11. Develop and implement facility-specific policies and procedures.</p>
<p><b>Audit of the CPSC'S Directives System (Directives)</b></p> <p>March 21, 2019</p>	<p>Directives-2. Update directives to ensure they align with directives system policies and procedures as well as reflect the current CPSC organizational structure and operations.</p>
<p><b>Review of Personal Property Management System and Practices for the Calendar Year 2017 (PMS)</b></p> <p>May 31, 2019</p>	<p>PMS-7. Develop and implement controls to ensure that the data entered into PMS and IFS is accurate and consistent with CPSC policies and procedures.</p> <p>PMS-8. Develop procedures to review applicable regulations and laws on an annual basis in order to ensure the property management policies and procedures remain accurate and complete.</p>

<i>Report Name and Date</i>	<i>Consolidated Recommendations</i>
<p data-bbox="224 1003 695 1167"><b>Review of Personal Property Management System and Practices for the Calendar Year 2017 (PMS)</b></p> <p data-bbox="224 1188 412 1222">May 31, 2019</p>	<p data-bbox="776 306 1341 407">PMS-9. Perform and document a formal analysis on the PMS operating environment and system mission to determine the appropriate system categorization for PMS.</p> <p data-bbox="776 436 1344 588">PMS-10. Upon a justifiable determination of the PMS system categorization, design, implement, and assess the PMS security controls and formally authorize PMS to operate in accordance with CPSC organizational security policies and procedures as well as other applicable government standards.</p> <p data-bbox="776 617 1344 743">PMS-11. Establish and implement POA&amp;M management procedures to ensure that all identified security weaknesses, including PMS application-specific and inherited control weaknesses, are fully documented and tracked.</p> <p data-bbox="776 772 1331 873">PMS-13. Establish and implement POA&amp;M management procedures to ensure that changes to estimated completion dates should be documented and reflected in the POA&amp;M tracker.</p> <p data-bbox="776 903 1305 953">PMS-14. Estimated completion dates should be documented and reflected in the POA&amp;M tracker.</p> <p data-bbox="776 982 1344 1083">PMS-15. Perform and document a formal analysis of PMS's operating environment and system mission to determine the appropriate risk level categorization for PMS.</p> <p data-bbox="776 1113 1321 1213">PMS-16. Upon a justifiable determination of PMS's system categorization, design and implement standard procedures for requesting and approving user access to roles and resources in PMS.</p> <p data-bbox="776 1243 1341 1394">PMS-17. Develop, approve, and implement procedures to ensure that standard users and administrators are included in the periodic review of PMS user access and that the custodian user access is validated appropriately when performing the review.</p> <p data-bbox="776 1423 1351 1495">PMS-18. Update the PMS Internal Control Document, or equivalent documentation, to reflect PMS's updated process.</p> <p data-bbox="776 1524 1351 1596">PMS-19. Complete and document the periodic review for all PMS users in accordance with PMS's updated procedures.</p> <p data-bbox="776 1625 1321 1696">PMS-20. Perform and document a risk analysis to identify SoD conflicts that may exist between PMS and other CPSC systems.</p> <p data-bbox="776 1726 1321 1827">PMS-21. Upon completion of the risk analysis, develop and implement procedures to ensure that CPSC users do not have unmonitored conflicting access across multiple systems.</p> <p data-bbox="776 1856 1312 1906">PMS-22. Perform and document a risk analysis to identify potential SoD conflicts within PMS.</p>

<i>Report Name and Date</i>	<i>Consolidated Recommendations</i>
<p><b>Review of Personal Property Management System and Practices for the Calendar Year 2017 (PMS)</b></p> <p>May 31, 2019</p>	<p>PMS-23. Upon the completion of the risk analysis noted above, management should develop and implement procedures that ensure PMS users do not have sufficient access to allow the unmonitored execution of incompatible transactions.</p> <p>PMS-24. Update and implement configuration change management procedures which include requirements to perform and document quality control reviews.</p> <p>PMS-25. Develop and implement procedures to log, track, and maintain a list of changes made to the PMS application.</p>
<p><b>Penetration and Vulnerability Assessment of CPSC's Information Technology Systems (PT)</b></p> <p>June 11, 2019</p>	<p>PT-1. REDACTED</p> <p>PT-2. REDACTED</p> <p>PT-7. REDACTED</p> <p>PT-12. REDACTED</p> <p>PT-13. REDACTED</p> <p>PT-17. REDACTED</p> <p>PT-18. REDACTED</p> <p>PT-20. REDACTED</p> <p>PT-29. REDACTED</p> <p>PT-32. REDACTED</p> <p>PT-33. REDACTED</p> <p>PT-35. REDACTED</p> <p>PT-36. REDACTED</p> <p>PT-38. REDACTED</p> <p>PT-39. REDACTED</p>
<p><b>AUDIT OF THE CPSC'S GRANTS PROGRAM</b></p> <p>September 25, 2020</p>	<p>GRANTS - 1. Implement and document awardee reporting requirements based on the results of the financial risk assessments.</p> <p>GRANTS - 2. Develop, implement, and document a procedure to formally reconcile Objective Review Committee individual scoring documentation to the summary document to identify any transcription and calculation errors prior to awarding a grant.</p> <p>GRANTS - 3. Ensure that the awardee goals, objectives, and performance measures approved by the CPSC include measurable standards.</p>

<i>Report Name and Date</i>	<i>Consolidated Recommendations</i>
<p data-bbox="224 1003 688 1066"><b>AUDIT OF THE CPSC'S GRANTS PROGRAM</b></p> <p data-bbox="224 1100 505 1134">September 25, 2020</p>	<p data-bbox="777 256 1349 331">GRANTS - 4. Ensure that the CPSC require awardees measure performance against outcomes as well as specific objectives.</p> <p data-bbox="777 359 1354 459">GRANTS - 5. Require awardees to report and relate financial and performance information using Office of Management and Budget-approved government-wide standard forms prior to approving disbursements.</p> <p data-bbox="777 487 1382 588">GRANTS - 6. Complete and implement grant monitoring policies and procedures which include prior notice and approval requirements for grant changes that are in accordance with Uniform Guidance.</p> <p data-bbox="777 615 1393 716">GRANTS - 7. Establish a process to thoroughly review financial information provided by grantees to ensure compliance with Virginia Graeme Baker Act requirements before approving payments.</p> <p data-bbox="777 743 1393 844">GRANTS - 8. Require invoices which include the dates goods and services are provided for all awards in order to substantiate that all costs were allowable and incurred within the award's Period of Performance.</p> <p data-bbox="777 871 1390 999">GRANTS - 9. Establish a process to require timely and complete reporting from Pool Safely Grant Program awardees. Such a process may include withholding the final award remittance until after all required reports are submitted.</p> <p data-bbox="777 1026 1362 1102">GRANTS - 10. Ensure grants management staff obtain timely written opinions from Office of General Counsel staff on issues of legal interpretation.</p> <p data-bbox="777 1129 1390 1283">GRANTS - 11. Obtain a written opinion from Office of General Counsel staff on the appropriateness of using VGB Act grant funds to pay for swimming lessons, whether such use violated the Purpose Act and, if a violation of the Purpose Act occurred, whether or not this violation constitutes an Anti-Deficiency Act violation.</p> <p data-bbox="777 1310 1393 1386">GRANTS - 12. Formalize and implement written directives and policies and procedures to govern the Pool Safely Grants Program.</p> <p data-bbox="777 1413 1382 1463">GRANTS - 13. Identify Pool Safely Grants Program roles and responsibilities in the formal directive.</p> <p data-bbox="777 1491 1349 1591">GRANTS - 14. Include specific grants governance responsibilities in all position descriptions and performance plans for persons with a role in the Pool Safely Grants Program.</p> <p data-bbox="777 1619 1382 1747">GRANTS - 15. Perform a second level review of the Pool Safely Grants Program information reported on USAspending.gov and reconcile this information to source documents prior to posting in order to confirm the information's accuracy.</p> <p data-bbox="777 1774 1365 1875">GRANTS - 16. Improve the VGB Act code definitions in the Management Information System Guide to limit ambiguity and post the updated Management Information System Guide on cpscnet.</p>

<i>Report Name and Date</i>	<i>Consolidated Recommendations</i>
<p><b>AUDIT OF THE CPSC'S GRANTS PROGRAM</b></p> <p>September 25, 2020</p>	<p>GRANTS - 17. Provide training on the updated Management Information System Guide to those who are likely to charge their time to VGB Act codes.</p> <p>GRANTS - 18. Provide training on the updated Management Information System Guide to those who are likely to charge their time to VGB Act codes.</p> <p>GRANTS - 19. Determine what grant costs qualify as administrative costs and charge them VGB Act funds.</p> <p>GRANTS - 20. Implement a cost accounting methodology to enable the CPSC to more accurately report on the costs associated with the VGB Act.</p> <p>GRANTS - 21. Ensure previous costs related to section 1405 of the VGB Act are charged to the correct appropriation.</p> <p>GRANTS - 22. Have Office of General Counsel provide a written determination of whether there are any Purpose Act or Anti-Deficiency Act violations related to any of the VGB Act administrative expenditures.</p>
<p><b>REPORT OF INVESTIGATION REGARDING THE 2019 CLEARINGHOUSE DATA BREACH</b></p> <p>Transmitted: September 25, 2020</p>	<p>BREACH- 1. Reconvene the BRT to assess the full extent of the breach, and base its response on the totality of the breach.</p> <p>BREACH- 2. Establish blanket purchase agreements for identity monitoring, credit monitoring, and other related services for data breach victims.</p> <p>BREACH- 3. Complete and publish a document describing lessons learned after the BRT completes its work related to this breach.</p> <p>BREACH- 4. Complete and document annual tabletop exercises. The tabletop exercises test the breach response plan and help ensure that members of the team are familiar with the plan and understand their specific roles. Tabletop exercises should be used to practice a coordinated response to a breach, to further refine and validate the breach response plan, and to identify potential weaknesses in the agency's response capabilities.</p> <p>BREACH- 5. Conduct an annual Breach Response Policy plan review.</p> <p>BREACH- 6. Establish and complete an annual schedule to review blanket purchase agreements for adequacy, complete and document the tabletop exercise, and publish the updated annual Breach Response Policy plan review.</p> <p>BREACH- 7. Develop and document a comprehensive crisis communication plan. This plan should include a process to ensure that there is an authoritative source for data related to any incident.</p> <p>BREACH- 8. The crisis communication plan should include annual tabletop exercises and annual plan reviews.</p> <p>BREACH- 9. The CPSC should document the results of each crisis communication plan annual tabletop exercise.</p>

<i>Report Name and Date</i>	<i>Consolidated Recommendations</i>
<p data-bbox="224 1003 708 1096"><b>REPORT OF INVESTIGATION REGARDING THE 2019 CLEARINGHOUSE DATA BREACH</b></p> <p data-bbox="224 1129 685 1163">Transmitted: September 25, 2020</p>	<p data-bbox="776 256 1334 331">BREACH-10. The CPSC should publish the resulting comprehensive crisis communication plan after any update.</p> <p data-bbox="776 361 1386 457">BREACH-11. Develop a process to ensure that all information reported to Congress and otherwise publicly reported is reviewed for accuracy and correctly contextualized and described.</p> <p data-bbox="776 487 1386 562">BREACH-12. Review all available data and establish an accurate identification of all data inadvertently released, internally and externally, from 2010 to 2019.</p> <p data-bbox="776 592 1377 667">BREACH-13. Obtain an independent review of a sample of Clearinghouse responses prior to 2010 to determine the need for an expanded scope of the review.</p> <p data-bbox="776 697 1386 823">BREACH-14. Establish policies and procedures to ensure that when the agency reports data related to a data breach or other violation of law or regulation, the reported data has been independently verified by a person outside of the responsible organization.</p> <p data-bbox="776 852 1380 949">BREACH-15. Establish a process for communicating and enforcing the implementation of recommendations previously agreed to by management, as required by law.</p> <p data-bbox="776 978 1370 1075">BREACH-16. Include successful implementation of OIG recommendations as a performance metric for Senior Executive Service employees and other senior management officials.</p> <p data-bbox="776 1104 1393 1306">BREACH-17. Implement a single data extraction tool to allow maximum functionality in searching multiple product codes while adequately blocking protected data from release. This tool should default to block ALL fields which may contain 6(b) information and PII data. This data tool must contain a standardized data dictionary to limit placement of restricted information to identified fields.</p> <p data-bbox="776 1335 1396 1432">BREACH-18. Once the new tool in Recommendation 17 is implemented, turn off and remove all other data extraction tools from the CPSC inventory of available IT tools.</p> <p data-bbox="776 1461 1396 1537">BREACH-19. Limit access to the underlying database and the data extraction tool to those with a bona fide need for access.</p> <p data-bbox="776 1566 1393 1663">BREACH-20. Create a searchable online public database with scrubbed Clearinghouse data to reduce the number of individual Clearinghouse information requests that are processed.</p> <p data-bbox="776 1692 1386 1873">BREACH-21. Require training for all Clearinghouse staff, up to and including the AED for EPHA, on the use and functionality of this new tool, procedures for responding to requests for information, and requirements to protect 6(b) information and PII data. Include this training as part of the onboarding for all Clearinghouse staff, up to and including the AED for EPHA.</p>

<i>Report Name and Date</i>	<i>Consolidated Recommendations</i>
<p><b>REPORT OF INVESTIGATION REGARDING THE 2019 CLEARINGHOUSE DATA BREACH</b></p> <p>Transmitted: September 25, 2020</p>	<p>BREACH-22. Annually update and require refresher training for all Clearinghouse staff on the use of the data extraction tool and policies and procedures for accomplishing Clearinghouse work, up to and including the AED for EPHA.</p> <p>BREACH-23. Develop, disseminate, provide training, and implement policies and procedures on how to use this new data extraction tool to all Clearinghouse staff, up to and including the AED for EPHA. These policies must include step-by-step instructions and checklists to aid staff in completing routine tasks. These policies must include guides and checklists for supervisory review of Clearinghouse staff work.</p> <p>BREACH-24. Require additional training for Clearinghouse supervisory staff, up to and including the AED for EPHA, on effective review of Clearinghouse staff output.</p> <p>BREACH-25. Annually update and require refresher training for Clearinghouse supervisory staff, up to and including the AED for EPHA, on the effective review of Clearinghouse staff output.</p> <p>BREACH-26. Develop, implement, and require training for all Clearinghouse staff, up to and including the AED for EPHA, on a tracking system to monitor Clearinghouse receipt and fulfillment of all Clearinghouse data requests.</p> <p>BREACH-27. Require supervisory review of all completed Clearinghouse data requests.</p> <p>BREACH-28. Use the data from the tracking system to develop and publish annual statistics related to the work of the Clearinghouse.</p> <p>BREACH-29. Require initial and annual refresher training for all staff on the importance of protecting 6(b) information and PII, including the rights of individuals and businesses, and how to recognize 6(b) information and PII in documents and how to securely handle this information.</p> <p>BREACH-30. Enforce Principle of Least Privilege and limit access to data on the P-drive to individuals with a bona fide "need to know."</p> <p>BREACH-31. Develop, implement, and require participation by all senior EXHR management staff in a training program on the values and benefits of an internal control system including a session on the statements of assurance process and its importance.</p> <p>BREACH-32. Determine, document, and implement a structure for the Clearinghouse.</p> <p>BREACH-33. Determine, document, and implement the role of the Freedom of Information Act Office in responding to Clearinghouse requests.</p> <p>BREACH-34. Require the Office of Human Resources Management (Human Resources) to provide consultation to ensure that the organizational structure in EPDSI</p>

<i>Report Name and Date</i>	<i>Consolidated Recommendations</i>
<p><b>REPORT OF INVESTIGATION REGARDING THE 2019 CLEARINGHOUSE DATA BREACH</b></p> <p>Transmitted: September 25, 2020</p>	<p>meets the current operational needs, meets span of control best practices, and perform a skills gap analysis. Human Resources will provide a written report of its findings.</p> <p>BREACH-35. Implement the recommendations from the Human Resources study.</p> <p>BREACH-36. Complete and document the results of a risk assessment of Clearinghouse operations.</p> <p>BREACH-37. Design, document, and implement control activities to respond to the results of the completed risk assessment process.</p> <p>BREACH-38. Develop and implement written guidance on the importance of the statements of assurance process and the related documentation requirements.</p> <p>BREACH-39. Ensure that activities fulfilling Clearinghouse data requests be made visible to management through the creation and use of a specific WebTA code based on a newly created Management Information System code.</p> <p>BREACH-40. Consider disciplinary action for the supervisors who did not accurately report the status of internal controls in the statements of assurance they produced. Document the results of the disciplinary review, to include the analysis supporting any decision to not perform disciplinary action.</p>

## CONTACT US

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



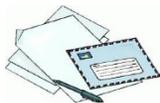
### **Call:**

301-504-7906  
1-866-230-6229



### **On-line complaint form:**

Click [here](#) for complaint form.  
Click [here](#) for CPSC OIG Website.



### **Write:**

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