



Office of Inspector General

U.S. Consumer Product Safety Commission

Consumer Product Safety
Improvement Act Annual Report
for Fiscal Year 2020

March 5, 2021

Report 21-O-04

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.



March 5, 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: Consumer Product Safety Improvement Act Annual Report for Fiscal Year 2020

The Consumer Product Safety Improvement Act of 2008 (CPSIA) requires that the Inspector General of the U.S. Consumer Product Safety Commission annually provide to the appropriate congressional committees the findings, conclusions, and recommendations from its reviews and audits performed under subsection 205(a) of the CPSIA as well as actions taken with regard to employee complaints under subsection 205(b). The attached report fulfills these requirements for fiscal year 2020.

Please feel free to contact me if you or your staff have any questions or concerns.

Abbreviations and Short Titles

CPSC	U.S. Consumer Product Safety Commission
CPSIA	The Consumer Product Safety Improvement Act of 2008
FISMA	The Federal Information Security Modernization Act
OIG	Office of Inspector General

Background

The Consumer Product Safety Improvement Act of 2008 (CPSIA) requires that the Inspector General of the U.S. Consumer Product Safety Commission (CPSC) annually report the findings, conclusions, and recommendations from its reviews and audits performed to meet the requirements of subsection 205(a) of the CPSIA. Specifically, subsection 205(a) instructs the Inspector General to assess the CPSC's capital improvement efforts, which includes upgrades of the information technology architecture and systems as well as the development of a publicly accessible website.

In addition, subsection 205(b) requires that the Inspector General review any employee complaints fitting the definitions set forth in CPSIA subsection 205(b) and actions taken by the CPSC to address them.

The CPSIA requires an annual report to the appropriate Congressional committees of the Inspector General's findings, conclusions, and recommendations from the reviews and audits under subsection 205(a) and complaints under subsection 205(b).

Assessment of CPSIA-Compliant Activities

Evaluation of CPSC's FISMA Implementation for FY 2020

(Click [here](#) for the full report)

The Federal Information Security Modernization Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency. It also requires that the relevant Office of Inspector General (OIG) perform an annual assessment of the agency's compliance with FISMA.

The OIG contracted with Williams, Adley & Company-DC, LLP, an independent public accounting firm, to perform a review of the CPSC's compliance with the FISMA reporting requirements for fiscal year 2020. The review was performed in accordance with the Council of the Inspectors General on Integrity and Efficiency Quality Standards for Inspections and Evaluations. The review focused on the CPSC's compliance with the FISMA metrics provided by the Department of Homeland Security and the Office of Management and Budget.

The contractor found that the CPSC was not compliant with all of FISMA's requirements. The CPSC's FISMA non-compliance has a direct impact on the confidentiality, integrity, and availability of the public facing database. However, the CPSC is making progress in implementing many of the FISMA requirements. The report contains 47 recommendations to improve the CPSC's information security posture.

Employee Complaints

No complaints fitting the definitions set forth in subsection 205(b) of the CPSIA were received by this office during fiscal year 2020. However, there was a complaint received in 2019 for which a Report of Investigation and associated recommendations were not issued until 2020. The CPSC has, to date, not addressed all of the recommendations made in that report.

Report of Investigation Regarding the 2019 Clearinghouse Data Breach (Click [here](#) for the full report)

On September 25, 2020, the OIG issued a report examining the CPSC's unauthorized release of sensitive information regarding thousands of people and businesses. We ascertained, among other findings, that the scope of the data breach was greater than previously reported and that the data breach was the result of incompetence and mismanagement rather than outside hackers gaining access to the CPSC's information technology systems.

The OIG agreed to investigate the CPSC's Clearinghouse data breach after receiving numerous requests from Congress and CPSC Commissioners. We initiated an administrative investigation to assess the scope, root causes, and the CPSC's response to the data breach as well as several specific allegations of misconduct, including whether the data breach was deliberate.

We quickly confirmed that the data breach was not the result of outside hackers gaining access to the CPSC's information technology systems. In fact, CPSC employees caused the data breach by inappropriately releasing confidential information. However, early on, we determined that the scope of the breach greatly exceeded the agency's estimate. We found:

- The inappropriate release of information began earlier and was of greater volume than believed by the agency.
- The root causes of the data breach were mismanagement and incompetence.

- The CPSC attempted to respond quickly to the breach. However, the CPSC's response to the breach was hindered by its lack of preparation for dealing with data breaches and the errors made in assessing the scope of the breach.
- No evidence that the data breach was deliberate.

The OIG had previously brought many of the issues that led to the data breach to management's attention; these problems were neither new nor unknown to the agency. Specifically, we had previously notified the agency about the lack of internal controls in the Clearinghouse, the lack of adequate encryption of personally identifiable information, and the failure to restrict access to non-public data to those with a need for this access.

Public Website Links

As of this writing, the homepage of the CPSC's website has an active link to the Inspector General's website. The OIG's website has methods for individuals to report cases of fraud, waste, and abuse regarding the CPSC.

CONTACT US

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



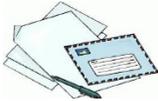
Call:

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