Office of Inspector General

U.S. Consumer Product Safety Commission

Report of Investigation Regarding the 2019 Clearinghouse Data Breach

September 25, 2020

20-ROI-01

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.

September 25, 2020

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

FROM: Christopher W. Dentel, Inspector General

SUBJECT: Clearinghouse Data Breach Report of Investigation

On April 1, 2019, the U.S. Consumer Product Safety Commission (CPSC) learned that a data breach involving the Clearinghouse had occurred. This data breach was not the result of outside hackers gaining access to the CPSC's information technology (IT) systems; CPSC employees caused the data breach by inappropriately releasing confidential information. Both senior management at the CPSC and members of Congress asked the Office of Inspector General (OIG) to investigate the Clearinghouse data breach. We agreed to assess the scope, root causes, and the CPSC's response to the data breach. We were also asked to investigate several specific allegations of misconduct.

The data breach was caused by a combination of mismanagement and incompetence. We found no evidence that that the data breach was deliberate. We determined that the scope of the data breach exceeded the CPSC's estimate in terms of both duration and quantity. 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 Clearinghouse, despite knowing this was not true.

The attached report of investigation contains 13 Findings and 40 Recommendations. When completed, these recommendations will significantly strengthen CPSC operations and better secure sensitive information within the Clearinghouse and across the agency as a whole.

Report of Investigation Regarding the 2019 Clearinghouse Data Breach

September 25, 2020 **Executive Summary**

Objective	**Assessment**
On April 1, 2019, Consumer Reports informed the U.S. Consumer Product Safety Commission (CPSC) that CPSC Clearinghouse employees had, while answering a routine Clearinghouse data request, provided Consumer Reports with restricted business information. The CPSC later learned that CPSC employees had also inappropriately provided restricted business information and Personally Identifiable Information (PII) to other entities in the course of responding to Clearinghouse data requests. The Inspector General Act of 1978, as amended, charges the Offices of Inspector General to conduct investigations relating to the programs and operations of their agencies and to recommend policies designed to promote economy, efficiency, and effectiveness of programs and operations. The primary objectives of this administrative investigation are to determine the scope and root causes of the Clearinghouse data breach and to assess the CPSC's response. The results of this investigation should assist the CPSC in identifying and prioritizing remedial efforts to prevent future data breaches, determine the scope of the breach, and assess what additional corrective actions to take. In addition to the above, the Office of Inspector General (OIG) was also asked to look into allegations that: there was collusion between CPSC employees and employees of Consumer Reports; the data breach was deliberate; the CPSC made threats against both Consumer Reports and CPSC employees; and the quality of the CPSC's response to the data breach was adversely affected by having employees who were responsible for the data breach in charge of responding to the data breach. (See below for Background)	The CPSC's initial assessment of the source of the data breach was correct. 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, the OIG determined that the scope of the breach greatly exceeded the agency's estimate. Therefore, the OIG contracted with forensic auditors to conduct an independent review of emails sent by CPSC Clearinghouse employees from 2010 through 2019 in order to determine the size of the data breach. We determined that the CPSC inappropriately released sensitive information to 556 recipients rather than the 29-36 recipients reported by the CPSC. According to our analysis, CPSC employees sent the 556 recipients a total of 1,725 emails, the majority of which involved transmitting PII and/or 6(b) protected data outside of the CPSC's domain without end-to-end encryption. These emails contained sensitive information, either restricted business information or PII. Section 6(b) of the Consumer Product Safety Act, the Privacy Act, or both, should have protected this information from release to unauthorized recipients. Additionally, both general federal requirements promulgated by the National Institute of Standards and Technology, as well as local CPSC Rules of Behavior, require that all transmissions containing sensitive information be encrypted if (Assessment continued below)

Background

Members of the public, businesses, stakeholders, other federal agencies, and agency employees are able to request information from the CPSC's Clearinghouse. What information is releasable can vary based on the requestor; for example, manufacturers can receive detailed reports about their own products. However, section 6(b) of the Consumer Product Safety Act generally prohibits the release of certain information about manufacturers to the public. Similarly, there are various prohibitions, including the Privacy Act, that prevent release of certain PII. Requestors generally receive information from the Clearinghouse by email; however, in the past, fax, CD ROMs sent through the United States Postal Service, and secure file transfer protocol solutions have also been used.

There is no formal organizational entity titled "Clearinghouse" in the CPSC. By law, the CPSC must "collect, investigate, analyze, and disseminate injury data, and information, relating to the causes and prevention of death, injury, and illness associated with consumer products." Clearinghouse is the term used to refer to these statutorily required duties. Clearinghouse is also a colloquial term used to describe the staff who complete the statutory duties described above. Clearinghouse tasks include the intake of new information from multiple sources and responding to requests for information from the public, manufacturers, and other governmental entities.

As part of its initial response to the data breach, the CPSC stated that the breach occurred from 2017 to 2019 and impacted approximately 30,000 people and 10,900 businesses. Both CPSC senior management and members of Congress requested that the CPSC OIG investigate both the data breach itself and the agency's response. Although the CPSC is still taking corrective actions in response to the Clearinghouse data breach, enough time has passed since the discovery of the breach that now seems an appropriate time to publish our report assessing the actions already taken and recommending additional corrective actions.

they are sent outside of the CPSC domain. In addition to the inadvertent release of 6(b) information and PII to entities external to the CPSC (such as Consumer Reports), there was also an internal component to the data breach. Hundreds of unauthorized employees had access to the unsecured shared drive containing 6(b) information and PII.

The primary causes of the data breach were mismanagement and incompetence. The mismanagement manifesting in the near total lack of properly designed and implemented internal controls and CPSC executive level employees demonstrating a lack of integrity regarding this lack of 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. The incompetence manifesting in the lack of: supervision, documented policies and procedures, and training for non-supervisory and first level supervisory Clearinghouse employees.

The OIG found no evidence that: there was collusion between CPSC employees and employees of Consumer Reports, the data breach was deliberate, or CPSC management made threats against either Consumer Reports or CPSC employees.

However, CPSC senior management relied on staff in charge of the Clearinghouse to assess the scope of the data breach. The methodology used to assess the data breach was not clearly documented and the individuals performing the assessment lacked both training and experience in dealing with data breaches. This resulted in a minimization of the scope of the data breach and compromised the CPSC's efforts to effectively respond to the data breach.

The OIG provided 40 actionable recommendations. When completed, these recommendations will significantly strengthen CPSC operations and secure sensitive information. Management has provided a written response which is included as an appendix to this report.

Table of Contents

List of Abbreviations

Acronym	Meaning
6(b)	Data protected under Section 6(b) of the CPSA
A-123	OMB Circular A-123 Management's Responsibility for Enterprise Risk Management and Internal Control
AED for EPHA	Assistant Executive Director for the Office of Epidemiology
AED for EXHR	Assistant Executive Director for Hazard Reduction
BRT	Breach Response Team
CIO	Chief Information Officer
CPS360	Consumer Product Safety Risk Management System
CPSA	Consumer Product Safety Act of 1972
CPSC	U.S. Consumer Product Safety Commission
CPSRMS	Consumer Product Safety Risk Management System
DED for OPS	Deputy Executive Director for Operations
EPDS	Data Systems Division
EPDSI	Data Intake Branch
EPHA	Office of Epidemiology
EPIR	Epidemiology Retrieval
EXHR	Office of Hazard Identification & Reduction
EXIT	Office of Information & Technology Services
FISMA	Federal Information Security Modernization Act of 2014
FMFIA	Federal Managers' Financial Improvement Act of 1982
FOIA	Freedom of Information Act
FY	Fiscal Year
GAO	Government Accountability Office
Green Book	*Standards for Internal Control in the Federal Government*
IDI	In-Depth Investigation
IT	Information Technology
KEARNEY	Kearney & Company
M	Memorandum
NCCIC	National Cybersecurity and Communications Integration Center
NEISS	National Electronic Injury Surveillance System
OCM	Office of Communications
OGC	Office of General Counsel
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
RMS360	Risk Management System 360
SAOP	Senior Agency Official for Privacy
SAS	Statistical Analysis System
SOP	Standard Operating Procedure

Request for Investigation

On April 1, 2019, the U.S. Consumer Product Safety Commission (CPSC) learned that a data breach involving the Clearinghouse had occurred. This data breach was not the result of outside hackers gaining access to the CPSC's information technology (IT) systems; in fact, CPSC employees caused the data breach by inappropriately releasing confidential information. In the course of responding to Clearinghouse requests for information, CPSC employees routinely failed to redact confidential information that should not have been released to the requestors. Although it was initially believed that the data breach was limited to information inadvertently released to Consumer Reports, it quickly became apparent that confidential information had been inappropriately released to a number of other requestors. The CPSC's assessment of the scope of the Clearinghouse data breach changed over time. Ultimately, the CPSC asserted that the data breach: had occurred between 2017 and 2019, involved 29-36 recipients who inadvertently received restricted business information relating to 10,900 businesses, and the personal information of approximately 30,000 individuals.

Both senior management at the CPSC and members of Congress asked the Office of Inspector General (OIG) to investigate the Clearinghouse data breach. We agreed to assess the scope and root causes of the data breach itself as well as the CPSC's response to the data breach. We were also asked to investigate several allegations:

- Was the data breach the result of either collusion between Consumer Reports and CPSC employees or in any other way a deliberate act?
- Did CPSC management threaten either Consumer Reports, in retaliation for publishing the information they received from the data breach, or individual CPSC employees for their roles in the data breach?
- Was the quality of the CPSC's response to the data breach adversely affected by having employees who were responsible for the data breach in charge of responding to the data breach?

Scope and Methodology

Scope

The initial scope of this investigation covered Clearinghouse operations from 2017 to 2019. This initial scope was based on the original request for investigation made to this office. After our initial work, we expanded the scope to all emails with

attachments sent outside the CPSC by employees of the Clearinghouse from January 1, 2010 to June 30, 2019.[1] The OIG quickly determined that employees had been fulfilling data requests long before 2010. However, the OIG limited the scope of the investigation to 2010 because that year the Clearinghouse moved from the Office of Information and Technology Services (EXIT) to the Office of Hazard Reduction (EXHR). Also, in 2010 there were technical changes made in the way Clearinghouse staff extracted data. That year Risk Management System 360 (RMS360), the current primary data extraction tool, replaced Epidemiology Retrieval (EPIR) as the official data extraction tool.

When the OIG chose to limit the scope of the investigation to "emails with attachments sent outside of the CPSC" we were aware that this scope did not capture all responses to data requests since 2010. As recently as a few years ago, employees were responding to data requests via fax, CD ROMs sent through the United States Postal Service, and secure file transfer protocol solutions. However, the CPSC maintained no records of the Clearinghouse's releases of information sent via any of these means of transmission. Additionally, given the total volume of email and the relatively low likelihood that employees manually entered confidential information into the text of emails (as opposed to including an attachment), emails that did not contain attachments were not reviewed.

Although our review primarily focused on inappropriately released information related to the Clearinghouse, we also found information that had been inappropriately released related to the operations of SaferProducts.gov. This occurred because, to a large extent, the same employees who worked on Clearinghouse matters also worked on SaferProducts.gov matters. SaferProducts.gov is a publicly available consumer product safety website operated by the CPSC.[2] The agency has been made aware of both the scale and scope of the inappropriate release of information related to SaferProducts.gov. As it is outside of the scope of our investigation, we will not address it in detail in this report. It is management's responsibility to determine how to appropriately deal with this data breach in accordance with Office of Management and Budget (OMB) Memorandum (M)-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*.

[1] Based on an allegation made by a witness, we also reviewed emails sent to certain specified addresses within the CPSC. However, no instances were found where the emails sent to the specified addresses were later forwarded outside of the agency, as alleged by the witness.
[2] Although there are exceptions to the protections generally offered by 6(b) for information that has been properly vetted and posted in the SaferProducts.gov database, these exceptions apply to the database itself. They do not apply to 6(b) protected information contained in emails sent while in the process of determining if information should be posted in the SaferProducts.gov database, and they do not apply to information protected by the Privacy Act, such as Personally Identifiable Information.

While SaferProducts.gov is outside the scope of this investigation, implementation of a number of the recommendations contained in this report could also increase data security for restricted business information as defined in section 6(b) of the Consumer Product Safety Act (CPSA) (subsequently referred to as 6(b) information) and Personally Identifiable Information (PII) contained on SaferProducts.gov.

Additionally, on or about March 20, 2019, an OIG staff member discovered unencrypted PDF files containing PII posted to the CPSC Freedom of Information Act (FOIA) webpage. The employee promptly reported this potential data breach to the CPSC Computer Security Incident Response Team. This incident was determined to constitute a data breach by the CPSC. Although the agency response to that data breach overlapped with the period covered by this investigation, that data breach and subsequent agency response are outside of the scope of this investigation.

Methodology

The OIG interviewed:

- 28 CPSC personnel with a role in sending out emails containing 6(b) information or PII or with knowledge of the causes of the breach or the CPSC's response
- 3 outside parties with information relevant to this breach

The OIG obtained and reviewed:

- the relevant laws and regulations to gain an understanding of requirements for Clearinghouse operations and data security
- internal CPSC policy and procedure documents to gain an understanding of Clearinghouse operations and data security measures
- IT security documents to gain an understanding of Clearinghouse IT systems
- prior audits and other reviews to gain an understanding of earlier concerns expressed to management
- the CPSC's progress in remediating issues identified earlier to gain an understanding of agency efforts to address prior OIG recommendations
- relevant statements of assurance to gain an understanding of agency management's perceptions concerning the strength of its internal control system

The OIG reviewed and re-performed the sampling methodology used by the agency to determine the scope of the data breach. Based on the above, it was determined

that the CPSC would need to seek an external assessment of the scope of the data breach.

The OIG obtained an independent forensic review of the 16,700 Clearinghouse emails sent during the relevant time period (January 1, 2010 - June 30, 2019) which met the criteria of having been sent by Clearinghouse employees to a non-CPSC email address with attachments.[3] The employees were identified by agency management as having performed Clearinghouse tasks during the relevant time period.

The OIG conducted an assessment of internal controls over the Clearinghouse based on the principles found in the Government Accountability Office (GAO), *Standards for Internal Control in the Federal Government* (Green Book).

Background

CPSC Mission

The CPSC is an independent agency created in 1972 by the CPSA, with a mission to protect consumers from unreasonable risks of injury or death associated with consumer products under the agency's jurisdiction. These products range from lawn mowers to cigarette lighters to baby strollers, and include items manufactured domestically and outside the United States.

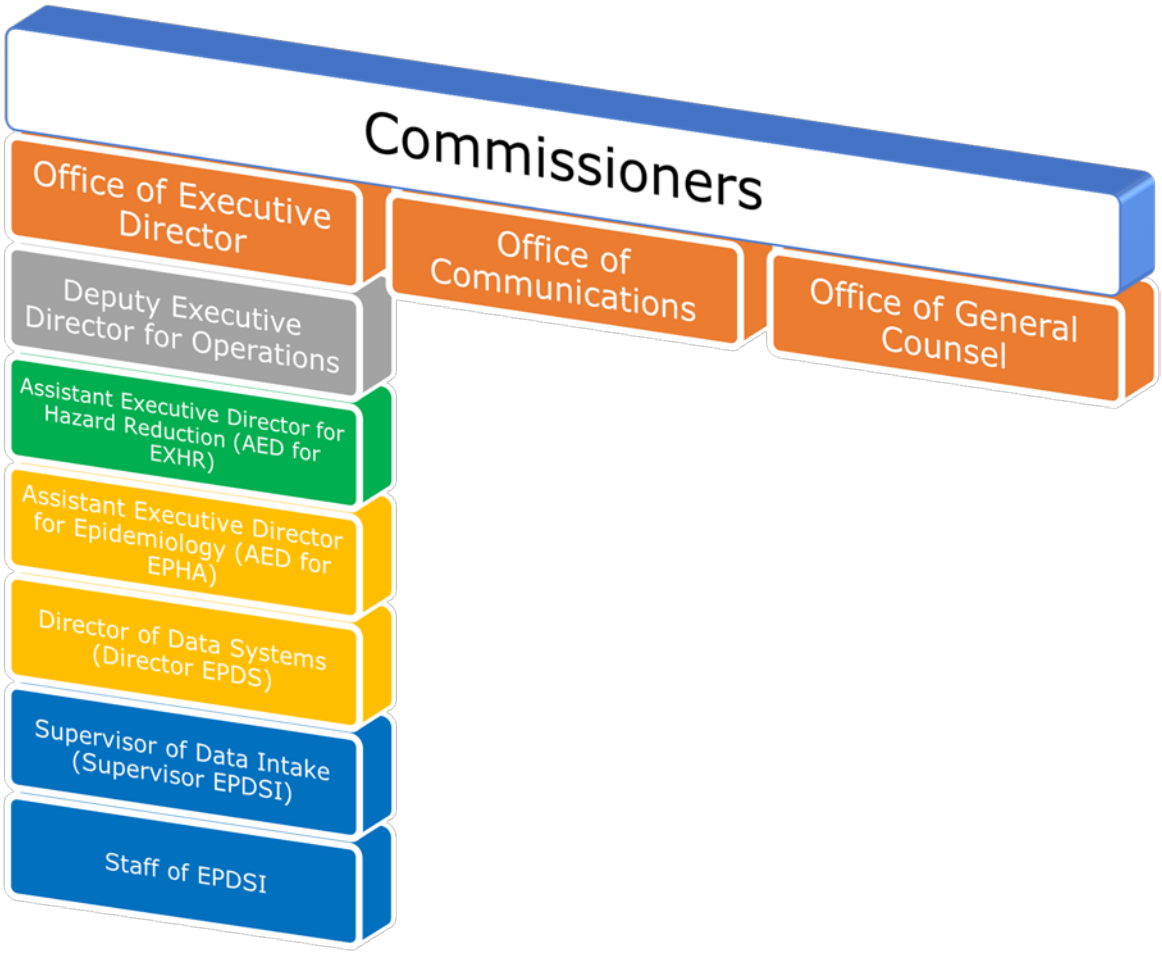
To accomplish this mission, the CPSC primarily works with relevant industry stakeholders and standards organizations, such as the American National Standards Institute, Underwriters Laboratories, and others to develop voluntary standards. The CPSC is also empowered under certain circumstances to issue mandatory standards, obtain recalls of products that need a specific repair, or even ban products, if necessary. The CPSC also researches potential product hazards and conducts campaigns to educate consumers about product safety. The CPSC maintains several databases containing information regarding potential product-related injuries under the framework of the National Injury Information Clearing-house.

The CPSC is subject to government-wide laws and regulations. As a federal agency, the CPSC is subject to the Federal Managers Financial Integrity Act of 1982

[3] Based on an allegation made by a witness, we also reviewed emails sent to certain specified addresses within the CPSC. However, no instances were found where the emails sent to the specified addresses were later forwarded outside of the agency, as alleged by the witness.

(FMFIA), the basis for internal control. The FMFIA requires managers to provide assurances that they have safeguarded funds, property, and other assets against waste, loss, unauthorized use, or misappropriation. Additionally, the CPSC is required to use GAO standards as found in the Green Book to design, implement, and operate internal controls to achieve its objectives related to operations, reporting, and compliance.

CPSC Organization[4]



Source: OIG summary of CPSC information

The CPSC is composed of a maximum of five commissioners, no more than three of whom may be of the same political party. The President, with the advice and consent of the Senate, appoints commissioners to seven-year terms. Commissioners do not serve at the pleasure of the President, and may only be removed for neglect of duty or malfeasance in office but for no other cause. The President, again with the advice and consent of the Senate, selects one of the

[4] Organizational chart reflecting only offices and positions related to the investigation.

commissioners to serve as Chairman. The CPSC Chairman is empowered to conduct the executive and administrative functions of the agency, including hiring and firing personnel, delegating duties among other commissioners and staff, and expending appropriations.

The current commissioners are:

- Acting Chairman Robert Adler – Democrat – Term expires October 2021
- Commissioner Dana Baiocco – Republican – Term expires October 2024
- Commissioner Peter Feldman – Republican – Term expires October 2026
- Commissioner Elliot Kaye – Democrat – Term expires October 2020

The Chairman delegates the executive and administrative functions of the agency to the Executive Director. Most offices report to the Executive Director; however, certain offices, including the Office of General Counsel (OGC) and Office of Communications (OCM), report directly to the Chairman.

The following positions and offices at the CPSC are relevant to this investigation. The Executive Director oversees the Deputy Executive Director for Operations (DED for OPS). The DED for OPS oversees the Assistant Executive Director for Hazard Reduction (AED for EXHR). The Deputy AED for EXHR oversees several offices, including the Office of Epidemiology (EPHA). The Assistant Executive Director for Epidemiology (AED for EPHA) oversees several divisions, including the Division of Data Systems (EPDS). The Director of Data Systems (Director for EPDS) oversees three branches, which contain a total of 33 positions: Data Intake (EPDSI), Statistical Support, and Data Operations. The supervisor of EPDSI, the branch that encompasses most Clearinghouse functions, supervises 13 employees.

Summary of the CPSC's Response to the Data Breach

The CPSC has records documenting the Clearinghouse's fulfillment of data requests going back to the mid-1990s. In 2010, the Clearinghouse was transferred from EXIT to EXHR. At that time, data requests were received via phone, fax, email, and US mail and answered via fax, CD ROMs sent through the United States Postal Service, and secure file transfer protocol solutions. Since 2010, Clearinghouse staff have fulfilled the majority of data requests via email with spreadsheets of information attached. On April 1, 2019, Consumer Reports contacted the CPSC and notified them that they had received restricted business information in a routine response to a data request. Senior management was notified and the AED for EPHA tasked his subordinates to determine the extent of the breach. They determined that 6(b) information had been inadvertently released to other

requestors in addition to Consumer Reports. The AED for EPHA presented his findings to senior management the following week.

Despite the Senior Agency Official for Privacy (SAOP) being informed on April 5, 2019, of the possibility that PII had been included in the data breach, the CPSC Breach Response Team (BRT) did not meet until April 16, 2019. From this point forward, the CPSC's response to the data breach was bifurcated. The agency continued to deal with the inadvertent release of 6(b) information by attempting to contact the recipients of the information and asking them to return or destroy the information. The CPSC relied upon the BRT to determine what course of action to follow in regards to the inadvertent release of PII. The BRT ultimately determined that the PII release was a minor incident and did not notify those impacted by the release.

The Executive Director tasked the AED for EPHA to look back to 2010 to determine how far back bulk disclosures of 6(b) information occurred. The AED for EPHA asserted to management that the data breach only extended back to 2017, and that the data breach occurred due to both a turnover in the personnel charged with responding to Clearinghouse data requests and a change in the methodology used for the tracking of data requests. The AED for EPHA and his staff identified the recipients of the inadvertently released 6(b) information and the approximately 10,900 impacted manufacturers. The agency began a 5-phased approach to respond to the breach:[5]

Table 1: Phased Responses

PHASE 1
Send initial notification to all identified manufacturers that an unauthorized disclosure occurred.
PHASE 2
Provide additional information to those manufacturers whose information was released to Consumer Reports.
PHASE 3
Provide additional information to those contacted in Phase 2 who have questions about the disclosures to Consumer Reports that were not answered in Phase 2.
PHASE 4
Send follow-up information to those manufacturers whose information was sent to recipients other than Consumer Reports.
PHASE 5
Provide additional information to those contacted in Phase 4 who have questions about the disclosures to other recipients that were not answered in Phase 4.

Source: OIG summary of CPSC information

[5] For further information regarding the phases see https://www.cpsc.gov/Business--Manufacturing/section-6b-information-disclosure.

The agency finished its phased response to recipients and manufacturers in August 2019, and conducted training on the protections afforded by section 6(b) to EPHA staff in September 2019.

Breach Chronology Summary

For ease of reference, the following timeline summarizes the sequence of key events that gave rise to this investigation. See Appendix A for the full chronology.

Table 2: Summary of Key Events in 2019

WEEK 1	
31-Mar	Consumer Reports requests meeting with the CPSC to discuss data that was emailed to them.
1-Apr	CPSC senior management learns that 6(b) information was emailed to Consumer Reports, contacts Consumer Reports and requests data be returned. Request is denied.
2-Apr	OGC staff notified of breach and drafts formal data recovery request.
3-Apr	Consumer Reports refuses formal CPSC OGC request to return 6(b) information.
5-Apr	Senior management requests full count of all inadvertent disclosures of information. The SAOP is notified by agency management of a potential release of PII.
WEEK 2	
10-Apr	The CPSC reports 29 separate inadvertent disclosures impacting 10,900 businesses and approximately 30,000 individuals. Staff identifies one disclosure prior to 2017.
11-Apr	OGC begins sending notices to 10,900 impacted businesses.
15-Apr	BRT activated.
WEEK 4	
26-Apr	CPSC staff request a "pull" of potential breach emails from archived data.
WEEK 5	
6-May	The CPSC informs Consumer Reports there was PII as well as 6(b) information in the emails sent to them.
7-May	BRT completes work.
9-May	Consumer Reports certifies destruction of PII.
WEEK 17	
31-Jul	All recipients have reportedly returned or destroyed 6(b) information and PII except Consumer Reports. Consumer Reports retained 6(b) information.

Source: OIG analysis of CPSC data

Results of Investigations

Allegations of Undue Consumer Reports Influence

The OIG investigated the allegation that the data breach was caused in whole or in part by collusion between Consumer Reports and CPSC employees. The OIG found no evidence of Consumer Reports colluding with or exercising undue influence over CPSC employees. The OIG did find evidence that a CPSC employee improperly provided information to Consumer Reports in a format that was not offered to other requestors. The format in question was one that had been used appropriately in the past to respond to Consumer Reports requests for information. However, it had been superseded by a new format. This same employee was responsible for numerous other disclosures of information to requestors other than Consumer Reports. The employee's actions regarding both Consumer Reports and the other requestors appear to represent incompetence and a lack of supervision rather than collusion, bias, or any other form of premeditation.

The OIG found:

1. No evidence to support this allegation and thus makes no recommendations.

Allegations of Intentional or Malicious Disclosures

The OIG investigated the allegation that the data breach was the result of employee malice or in any other way premediated. The OIG found no evidence of any deliberate intent or premeditation regarding the data breach.

The OIG found:

2. No evidence to support this allegation and thus makes no recommendations.

Allegations of Threats

The OIG investigated allegations that CPSC management made threats against Consumer Reports, in retaliation for publishing the information they received as a result of the data breach, and toward individual CPSC employees, for their roles in the data breach. The OIG found no evidence of CPSC management making threats against either Consumer Reports or CPSC employees; nor did either Consumer Reports or CPSC employees report that they had been the recipient of threats. A number of the CPSC employees that we interviewed were anxious about our investigation and/or their potential culpability in the data breach – but they did not allege that anyone had threatened them.

The OIG did determine that the former AED for EXHR contacted the Director of Product Safety at Consumer Reports, and asked him not to release the information Consumer Reports had received as part of the data breach. The Director of Product Safety at Consumer Reports responded that the matter was with the Consumer Reports Office of General Counsel and was out of his hands. Neither the Director of Product Safety at Consumer Reports nor anyone else we interviewed from Consumer Reports alleged that they had been threatened or were aware of anyone at Consumer Reports who had been threatened. The former AED for EXHR denied threatening the Director of Product Safety at Consumer Reports or anyone else.

The OIG found:

3. No evidence to support this allegation and thus makes no recommendations.

The CPSC's Response to the Data Breach

The CPSC's response to the data breach was largely bifurcated based on the nature of the data inadvertently released and when the CPSC became aware of the inadvertent release. Initially, the CPSC was only aware of the 6(b) information inadvertently released to Consumer Reports. The CPSC was only aware that a 6(b) data breach had occurred because Consumer Reports notified the CPSC that it had received data from CPSC staff that included manufacturer-specific material which should have been redacted. CPSC staff requested that Consumer Reports return the data and destroy any copies; Consumer Reports refused.

The Executive Director was concerned 6(b) information might have been inadvertently disclosed to other requestors in addition to Consumer Reports. Because of this concern, she asked the DED for OPS to look at the nature of the Consumer Reports data request and what data was sent in response. He, in turn, consulted with the AED for EPHA, the official ultimately responsible for assessing the scope of the data breach. The AED for EPHA had his team look into the scope of the problem to try to determine if requestors other than Consumer Reports had received 6(b) information. They determined that other requestors had received 6(b) information. At this point, the CPSC began efforts to contact those recipients and request that they return or certify destruction of the 6(b) information.

Later, the CPSC became aware that some of these inadvertent disclosures of information included PII. This led to the activation of the BRT on April 15, 2019, 15 days after the agency was notified of a data breach, and 10 days after the SAOP was notified that PII had been released. Up until this point, the CPSC had directed all of its efforts at dealing with the unauthorized disclosure of 6(b) information.

Due to growing concerns that Clearinghouse staff were not competent to properly review and redact information, CPSC management announced OGC staff would review all future responses to requests for Clearinghouse information before release. This decision was characterized as temporary. This investigation did not assess the effectiveness of the OGC's efforts in this area.[6]

Breach Response Policy and Breach Response Team

In a memorandum dated May 7, 2019, the Chief Information Officer (CIO) of the CPSC, who as the SAOP served as the Chair of the BRT,[7] stated that on April 5, 2019, he was notified that PII was released in the data sent to Consumer Reports and others. As required by the Federal Information Security Modernization Act of 2014 (FISMA) and OMB M-17-12 the CPSC activated the BRT on April 15, 2019. The BRT held its first meeting on April 16, 2019. The BRT identified 99 files potentially containing PII sent during the period March 2017 – March 2019.[8] The BRT determined that those 99 files contained approximately

[6] As of the date of this report OGC is still reviewing responses to requests for Clearinghouse information. However, responses to voluntary standards groups and internal customers did not always receive OGC review.

[7] OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information,* defines a breach response team as "the group of agency officials designated by the head of the agency that may be convened to respond to a breach" and requires that at a minimum the BRT include: the SAOP, the CIO or designee, Senior Agency Information Security Officer, legal counsel, legislative affairs counsel, and communications official.

[8] Although much of the CPSC's reporting regarding the data breach involved the number of recipients of the data, at various times cited as being between 29-36, the BRT never specified the number of

30,000 records with PII. As part of their initial effort to deal with the inadvertent disclosure of 6(b) information, CPSC staff had already received confirmation of the destruction of over 28,000 of those records.

The BRT evaluated the potential impact of the inadvertently released PII using the National Cybersecurity and Communications Integration Center (NCCIC) tool, Cyber Incident Scoring System. The resulting score of 15 (out of a maximum of 100) for this incident is, according to the NCCIC scoring guidelines, a negligible impact. Although the CPSC had the authority to take corrective actions, such as notifying the impacted individuals or offering credit monitoring services, based on the NCCIC score of 15 the agency was not required to do so.[9] OMB M-19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, provides the definition for agencies to use in determining when a "major incident" has occurred as a result of a privacy breach. OMB guidance states, a major incident determination is required for any unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to the PII of 100,000 or more people. The BRT determined that the breach was, ". . . non-major and there was a low risk of harm to potentially affected individuals."[10] The CIO, with the concurrence of the BRT, recommended that the CPSC not notify individuals potentially affected by the breach.

The efforts of the BRT to evaluate the potential impact of the Clearinghouse data breach and to advise the CPSC on a course of action were compromised. The BRT was unaware that the breach extended back to at least 2010, rather than 2017. They were also unaware that in addition to the external component of the data breach, there was an internal component. This internal component consisted of the large number of individuals within the CPSC who had access to the shared drive containing the PII of consumers who had been injured by consumer products despite having no "need to know" this information. See sections on "Principle of Least Privilege" and "Design and Implement Information Systems Controls." As a result, the BRT assessed only a fraction of the total PII involved in the breach.

recipients of the data, instead their reporting focused on the number of files inadvertently released which they cited as 99.

[9] For additional information on scoring guidelines and factors, see https://www.us-cert.gov/CISA-Cyber-Incident-Scoring-System.

[10] Memorandum dated May 7, 2019, from the CIO of the CPSC, who as the SAOP served as the Chair of the BRT, to the CPSC's Acting Chairman.

The OIG found:

4. The BRT had incomplete information at the time of its breach review in 2019.
5. The CPSC did not comply with its Breach Response Policy, specifically the CPSC has not:
   - maintained the required identity and credit monitoring as well as related services
   - tracked, documented, and disseminated a lessons learned report from this breach
   - completed an annual tabletop exercise
   - completed an annual plan review

The OIG recommends CPSC management:

1. Reconvene the BRT to assess the full extent of the breach, and base its response on the totality of the breach.
2. Establish blanket purchase agreements for identity monitoring, credit monitoring, and other related services for data breach victims.
3. Complete and publish a document describing lessons learned after the BRT completes its work related to this 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.
5. Conduct an annual Breach Response Policy plan review.
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.

Messaging to the Public

An important part of the CPSC's response to the data breach was the messaging to the business community, public, and Congress. The situation and the information available were fluid; especially during the first few days following the discovery of the data breach. The CPSC began to provide counts of the recipients of the inadvertent disclosures and the impacted businesses as early as the first week of April 2019. Phase 1 of the data breach response began on April 11, 2019, predicated on 29 recipients and approximately 11,000 affected businesses.

The Director of Communications stated that he never directly spoke with the AED for EPHA about the scope of the data breach, but instead spoke only to the Executive Director. Over time, the CPSC's understanding of the total numbers of recipients of the inadvertently disclosed information and impacted businesses changed as additional information came to light. However, it does not appear that the CPSC had a documented strategy to keep Congress and the public informed of the changes in a timely manner. In fact, the Senate Commerce Committee report, published in October 2019, based on interviews conducted July 31, 2019, continued to reference the initial figure of 29 recipients of the inadvertent disclosures.[11]

Further, the public messaging did not disclose key facts about the number and nature of the published number of breaches. The number of disclosures reported during that time did not include disclosures of PII from the Clearinghouse nor did they include disclosures of one or two items of 6(b) information to a single recipient.

The OIG found:

6. The CPSC did not present a consistent and accurate message to the public and members of Congress.

[11] U.S. Senate Committee on Commerce, Science, & Transportation, "CPSC Section 6(B) Data Handling," Prepared by Commerce Committee Majority Staff, October 2019.

The OIG recommends CPSC management:

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.
8. The crisis communication plan should include annual tabletop exercises and annual plan reviews.
9. The CPSC should document the results of each crisis communication plan annual tabletop exercise.
10. The CPSC should publish the resulting comprehensive crisis communication plan after any update.

Result of the CPSC's Assessment of the Scope of the Data Breach

On April 5, 2019, the Executive Director requested a "full count" of unauthorized disclosures related to the Clearinghouse data breach. Rather than assigning staff from OGC or EXIT who were not involved in the operations of the Clearinghouse and have expertise in the Privacy Act, data beaches, and IT systems; the decision was made to place staff who bore some level of responsibility for the data breach in charge of assessing the scope of the data breach. On April 10, 2019, the AED for EPHA, a person responsible for oversight of the Clearinghouse, informed the Executive Director that he had identified the "universe of disclosure." However, it was not until April 26, 2019, 16 days later, that the AED for EPHA first asked EXIT staff to pull Clearinghouse emails with attachments for his review to determine the scope of the breach.

During April and May of 2019, the CPSC's focus was on what they described as "bulk disclosures" of 6(b) information. Bulk disclosures are email attachments which included significant numbers of lines of data or in some cases the entire database. The methodology, criteria, and results of this review were poorly documented. It is more likely than not that if attorneys from OGC or staff from EXIT with experience dealing with data breaches, the Privacy Act, and PII issues had been assigned to assess the scope of the data breach the analysis would have included PII and been more professionally conducted and documented.

It took the CPSC three attempts to find all the bulk 6(b) disclosures they ultimately publicly reported. In the first attempt, CPSC staff reviewed information contained in the EPDSI Information Request Tracking Spreadsheet. This spreadsheet was designed to be the master list of all fulfilled Clearinghouse requests and has been

used since October 19, 2016. Based on this work, the CPSC identified 29 unique recipients who received 51 unique email attachments. CPSC staff reported this information to management on May 6, 2019.

However, after comparing tracking sheet information to other sources, CPSC staff determined that not all fulfilled Clearinghouse requests were recorded on the tracking sheet. As a result, CPSC staff searched the email folder that each responder was meant to cc when responding to Clearinghouse requests. Based on this work, the CPSC identified four additional unique recipients of bulk disclosures and an additional seven unique email attachments. CPSC staff reported this information to management on May 13, 2019.

CPSC staff were still concerned that they had not identified all possible bulk disclosures. They ordered and reviewed a pull of 14,022 emails with attachments sent by Clearinghouse staff. Based on this work, the CPSC identified 3 additional unique recipients of bulk disclosures and an additional 12 unique email attachments. CPSC staff reported this information to management on May 22, 2019.

On July 1, 2019, OIG investigators asked the AED for EPHA to provide support for the "full count" of disclosures reported by the agency. Clearinghouse staff provided a spreadsheet that identified the 14,022 emails included in their population for review. Of those 14,022 emails, 4,975 were sampled. The results of this work were summarized in an Excel spreadsheet file with one sheet for each tranche of data pulled and a summary sheet. These sheets contained the subject line of each of the 14,022 emails pulled and outcome notations for most of the sampled emails. At the time of the interview, OIG staff were told that this was the underlying methodology for identifying what was characterized as inadvertent disclosures of 6(b) information. However, over the course of subsequent interviews it has become clear that these sheets did not present a complete picture of the methodology used to identify disclosures nor the limitations on the scope of the CPSC review.

The OIG review of the data raised some questions about the completeness of the data reported and the adequacy of the sampling completed. As a result, the OIG hired a forensic accountant to do a 100 percent review of emails with attachments sent by Clearinghouse staff to non-CPSC addresses to determine the full scope of the breach.

The OIG found:

7. The quality of the CPSC's response to the data breach was adversely affected by having employees who were responsible for the data breach in charge of responding to the data breach. The CPSC relied on incomplete and incompletely explained data in its reporting to the public.

The OIG recommends CPSC management:

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.

OIG Independent Review of the Scope of the Data Breach

After the OIG review of the CPSC's assessment of the data breach, questions persisted about its methodology, accuracy, and completeness. In an attempt to obtain a more accurate picture of the size of the breach, the OIG retained an independent firm, Kearney & Company (Kearney), to assess the scope of the breach by reviewing 100 percent of the emails with attachments sent outside the CPSC domain by Clearinghouse staff from January 1, 2010 to June 30, 2019. The majority, but by no means all, of the violations found involved transmitting PII and and/or 6(b) protected data outside of the CPSC's domain without the use of end-to-end encryption – a violation of both the CPSC's and federal requirements regarding securing sensitive information.[12] (See OMB Circular A-130, National Institute of Standards and Technology 800-53, SC-8, SC-13, and CPSC Rules of Behavior)

Below is the text of the results of Kearney's review:

> The scope of our work included an analysis of 16,700 emails with attachments originating from 45 personnel identified by the Office of Inspector General (OIG) who constituted a targeted sample of CPSC staff known to have worked in the Data Intake Branch of EPI [EPDSI] during the period January 1, 2010, through June 30, 2019. These emails were delivered to us from OIG staff via a secure data transfer system.

[12] The CPSC's assessment of the scope of the data breach did not include unencrypted emails containing PII or 6(b) protected information.

The purpose of this review was to identify all potential releases of PII and 6(b) information by Data Intake Branch staff to outside parties during the period in question. The population included emails with attachments sent outside of the organization to non-CPSC.gov email addresses as well as emails with attachments sent to specified addresses within the agency. We did not review processes or internal controls related to the Clearinghouse or other Data Intake Branch programs.

Kearney designed our procedures to identify instances of spillage of PII and "6(b)" information outside the CPSC network from the population provided by OIG. We developed an artificial intelligence algorithm (AI tool) to review the entire population. We verified the accuracy of our AI tool by a human review of a sample of reviewed emails, including those emails initially found to not contain any PII and 6(b). We recalibrated the AI tool based on our reviews of the results and reran the AI tool to provide the most accurate results.

Results

Based on our analysis of 16,700 emails, we determined that 4,527[13] emails contained PII and/or "6(b)" information. These included emails both prior to and after 2017. Additionally, emails containing this information were primarily sent in support of Clearinghouse and Safer Product information requests.

Table 3: Summarized Results of Analysis

PII Only Violations Found	"6b" Only Violations Found	PII and "6b" Violations Found	Total
341	910	474	1,725

Source: Kearney review of CPSC data

Kearney was able to provide information categorizing the violations as occurring before or after the implementation of the EPDSI Information Request Tracking Spreadsheet on October 19, 2016. This categorization was used because one of management's explanations for the inadvertent releases of information that occurred in 2017-2019 was that the change in the tracking method led to the data breach. However, as is evident below, the change in the tracking spreadsheet was irrelevant as there were disclosures before the new spreadsheet was implemented.

[13] This figure contains violative emails related to both the Clearinghouse and SaferProducts.gov. Based on the CPSC's assertion that they will treat the issues related to SaferProducts.gov as a separate data breach from the one involving the Clearinghouse we have excluded those emails from our analysis.

Table 4: Number of Disclosures by Date Range

Date Range	Emails Reviewed	PII Violations	6b Violations	PII and 6b Violations
January 1, 2010 - October 19, 2016	13,562	199	712	384
October 20, 2016 - June 30, 2019	3,138	142	198	90
Total	**16,700**	**341**	**910**	**474**

Source: Kearney review of CPSC data

Table 5: Number of Recipients* by Date Range

Date Range	Emails Reviewed	PII Violations	6b Violations	PII and 6b Violations
January 1, 2010 - October 19, 2016	13,562	78	265	98
October 20, 2016 - June 30, 2019	3,138	42	70	3
Total	**16,700**	**120**	**335**	**101**

*Unique email addresses
Source: Kearney review of CPSC data

The forensic auditors also provided the OIG with samples of the information transmitted. The items included an infant's unredacted death certificate and graphic medical PII regarding injuries to and/or deaths of children, including babies.

The OIG found:

8. The CPSC relied on and reported incomplete and inaccurate data and did not perform adequate due diligence and oversight of the work of Clearinghouse staff in reporting breach statistics.

The OIG recommends CPSC management:

12. Review all available data and establish an accurate identification of all data inadvertently released, internally and externally, from 2010 to 2019.

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.
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.

Root Causes

Prior Audit Results and Unaddressed Recommendations

As part of the investigation, the OIG reviewed its database of prior unimplemented recommendations to determine whether this data breach could have been reasonably anticipated and prevented. 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. Previous audits had already put the agency on notice of deficiencies in how the Clearinghouse processed information requests. The agency had been notified of the following issues and, with one exception, failed to address them:

Lack of Internal Controls in the Clearinghouse Program

In the 2015 Audit of the Freedom of Information Act Program report,[14] the CPSC OIG found that there was a lack of internal controls over In-Depth Investigation (IDI) requests. The report notes that:

> The CPSC's Clearinghouse Management has not developed written procedures to ensure the proper processing of requests for IDI Reports . . . Further, Management has not provided guidance nor performed supervisory review over work performed by the Clearinghouse Program Analysts.

[14] Link to 2015 FOIA report.

The OIG recommended the following:

> Therefore, we first recommend that the Program Analysts responsible for completing IDI requests in the Clearinghouse are included in the structured annual FOIA training program.
>
> Following the completion of the training, we recommend that the Clearinghouse with the assistance of the General Counsel Office of the Secretary develop a SOP [Standard Operating Procedure] to ensure that the receipt, processing, and tracking of FOIA requests for IDI files is accomplished in accordance with the FOIA legislation.

The agency concurred and agreed to implement these recommendations. As of the date of this report they have only implemented one.

Encryption of PII

The 2011 FISMA report noted problems and inconsistencies with encryption protocols related to emails sent from the CPSC:[15]

> The agency has a policy that requires all sensitive information to be encrypted prior to being sent outside of the internal network; however, the agency has not implemented a tool to facilitate compliance with this requirement. Therefore, there is an extremely high likelihood that users send unencrypted, sensitive files over public networks.

Recommendations in the 2011 FISMA report included that the CPSC:

> Implement a tool (e.g., Accel[li]on) to allow agency resources to encrypt sensitive documents prior to transmission across a public network, and train users of the tool. Perform periodic audits to ensure compliance with the policy of encrypting sensitive documents prior to transmission across a public network.

The agency's response to this recommendation was that they would not implement email encryption because of the potential for latency and difficulty with encryption key management. Again, in the 2012 FISMA report,[16] the OIG found:

[15] Link to 2011 FISMA report.
[16] Link to 2012 FISMA report.

> The agency also has a policy, which requires users to encrypt all sensitive information prior to transmitting the information outside of the internal network. However, although the agency has implemented a tool to facilitate compliance with this requirement in [Fiscal Year] FY 12, management has not configured the CPSC email solution to systematically encrypt emails prior to transmission across a public network. Also, management does not perform audits to ensure all sensitive emails and attachments transmitted across a public network utilize the encryption tool appropriately. Therefore, although the process has improved with the implementation of the encryption tool, an extremely high likelihood remains that users send unencrypted, sensitive files over Public networks.

Based on the information above, the OIG recommended in the 2012 FISMA report:

> Management should implement a solution to systematically require the encryption of all sensitive information transmitted across a public network, or periodically audit emails and attachments traversing a public network to ensure policy compliance, or implement a data loss prevention solution.

The agency concurred and agreed to implement these recommendations. As of the date of this report they have not implemented either.

Principle of Least Privilege

There have been concerns regarding access to the Consumer Product Safety Risk Management System (CPSRMS) since at least 2013. The 2013 FISMA Report[17] discusses the Principle of Least Privilege:[18]

> The agency has not implemented the Principle of Least Privilege for CPSRMS or cpsc.gov. All CPS360[19] (a CPSRMS subsystem) users can view all incident reports, even those that management has not approved for public consumption, whether or not their job function requires access to these data views. Additionally, management has not implemented roles within cpsc.gov or developed a workflow within

[17] Link to 2013 FISMA report.
[18] The Principle of Least Privilege, an important concept in computer security, is the practice of limiting access rights for users to the bare minimum permissions they need to perform their work. Under the Principle of Least Privilege, users are granted permission to read, write, or execute only the files or resources they need to do their jobs: in other words, the least amount of access necessary.
[19] The term CPS360 refers to the same system later referred to as RMS360.

cpsc.gov to require approval from management to publish content to the CPSC website. All users who have access to author content on cpsc.gov have sufficient access to publish without further adjudication.

In the 2013 FISMA report, the OIG recommended that management should restrict access to the non-public data housed in CPSRMS to users with a business need for this access.

The agency concurred and agreed to implement this recommendation. As of the date of this report they have not implemented it.

Table 6: Recommendations Previously Agreed to by Management

Report	Recommendation Number	Recommendation	Status
FOIA 2015	3	Therefore, we first recommend that the Program Analysts responsible for completing IDI requests in the Clearinghouse are included in the structured annual FOIA training program. The training should include education on the FOIA, the CPSC's FOIA procedural requirements, and when and how to properly assess fees for FOIA records.	OPEN
FOIA 2015	4	Following the completion of the training, we recommend that the Clearinghouse with the assistance of GCOS develop a SOP to ensure that the receipt, processing, and tracking of FOIA requests for IDI files is accomplished in accordance with the FOIA legislation.	CLOSED
FISMA 2011	17	Implement a tool (e.g., Accel[li]on) to allow agency resources to encrypt sensitive documents prior to transmission across a public network, and train users of the tool.	OPEN
FISMA 2011	18	Perform periodic audits to ensure compliance with the policy of encrypting sensitive documents prior to transmission across a public network.	OPEN
FISMA 2012	3	Management should implement a solution to systematically require the encryption of all sensitive information transmitted across a public network. Or periodically audit emails and attachments traversing a public network to ensure policy compliance. Or implement a data loss prevention (DLP) solution.	OPEN
FISMA 2013	9	Management should implement the Principle of Least Privilege for the GSS LAN.	OPEN

*Source: OIG recommendation tracking database

Over the course of the last eight years, management has made no satisfactory effort to address or resolve five of these six recommendations. Management's failure to adequately address these recommendations greatly aggravated the impact of the data breach. These recommendations are still unresolved even after the data breach.

The OIG found:

9. The CPSC has a history of concurring with but not promptly implementing audit recommendations.

The OIG recommends CPSC management:

15. Establish a process for communicating and enforcing the implementation of recommendations previously agreed to by management, as required by law.
16. Include successful implementation of OIG recommendations as a performance metric for Senior Executive Service employees and other senior management officials.

Clearinghouse Operations

The CPSC is required by law to maintain a Clearinghouse[20] to "collect, investigate, analyze, and disseminate injury data and information, relating to the causes and prevention of death, injury, and illness associated with consumer products." Clearinghouse is also the colloquial term used by the CPSC to describe the dissemination of injury data function within EPDSI. Despite the above, there is no formal entity at the CPSC titled "Clearinghouse"; instead, the term refers to those who perform the tasks associated with the Clearinghouse function. Clearinghouse tasks include the intake of new information from multiple sources and responding to requests for information from the public, manufacturers, and other governmental entities. Processing Clearinghouse requests is one of several functions performed by the staff of EPDSI using the data extraction tools described in more detail below.

[20] 15 U.S.C. § 2054(a).

Clearinghouse Information Requests

The CPSA created a statutory framework for the dissemination of injury data, and information relating to the causes and prevention of death, injury, and illness associated with consumer products. This statutory framework is unique to the CPSC. However, the CPSC, like most other federal agencies, is also subject to the FOIA.[21] Members of the public, businesses, stakeholders, or internal agency employees, are able to request information from the Clearinghouse. Clearinghouse requests can be for summarized records (usually a line of data for each incident), manufacturer reports, and IDI reports. Information requests are submitted via telephone, email, US mail, and FOIA request.

Prior to the data breach, EPIR and RMS360 were both used to search data to answer Clearinghouse requests. What information is releasable can vary based on a number of different factors. For example, manufacturers can receive details about their own products that would not be released to their competitors and individuals who request copies of reports related to themselves will not have their own PII redacted. Currently, email is the normal way of transmitting responses; however, in the past, requests were answered via US mail, fax, and CD ROM. When the request for information was part of a FOIA request, the responsive records were sent to the agency FOIA office for redaction and the FOIA office responded to the requestor. Prior to the data breach, a request for information from the Clearinghouse that was not part of a FOIA request, was redacted by EPDS staff who were also responsible for responding to the requestor. The information provided to all requestors is subject to the requirements of section 6(b) and the Privacy Act.

Data Sources and Extraction Tools

The Clearinghouse consists of data compiled from multiple sources including the National Electronic Injury Surveillance System (NEISS).[22] Other sources include: death certificates provided to the CPSC by state health departments when the cause of death involves consumer products; IDI files containing summaries of reports of investigations into events surrounding product-related injuries or incidents; and Injury/Potential Injury Incident files containing summaries of hotline

[21] 5 U.S.C. § 552.

[22] NEISS is comprised of a sample of hospitals that are statistically representative of hospital emergency rooms nationwide. Data is collected on a broad range of injury-related issues, covering hundreds of product categories, and provides national estimates of the number and severity of product-related injuries. The data is then scrubbed and placed on a public searchable database on https://www.cpsc.gov/cgibin/NEISSQuery/home.aspx.

reports indexed by consumer product, product-related newspaper accounts, reports from medical examiners, and letters to the CPSC.

Historically, when the CPSC received a request for Clearinghouse information, an employee from EPDSI had several tools available to extract the information from CPSRMS necessary to reply to the request. Before 2010, the Clearinghouse used Statistical Analysis System (SAS), a commercial off-the-shelf solution, and EPIR, an in-house developed data retrieval application, to extract data.

The primary tool prior to 2010, EPIR, defaults to a public release view and removes 6(b) information and PII. However, EPIR is slow and prone to crashing. Also, EPIR can only search two product codes at a time; thereby limiting the search results. Employees who know SAS can use it within EPIR to increase search speed and run searches with more than two product codes. However, using SAS requires extra steps on the part of staff when inputting queries.

RMS360 was developed to replace EPIR and resolve its product code limitations. RMS360 searches an unlimited number of product codes. However, this capability came with trade-offs. While EPIR can search on the date of death, incident date, or report date, RMS360 only searches on the incident or report date. For example, because RMS360 could only search the incident or report date, if a person was injured one day, but died six months later, that case would not appear in an RMS360 search result looking for deaths related to that product. Therefore, the choice of one data extraction tool over another could result in different data results for a search request. Because of these limitations EPIR was never decommissioned.

Additionally, unlike EPIR which defaults to only show information releasable to the public, RMS360 does not have any automated controls in place to prevent the release of 6(b) information and PII. In fact, RMS360 defaults to releasing 6(b) information and PII. Thus, Clearinghouse staff who answer IDI requests using RMS360 have to manually go through the data to attempt to prevent 6(b) information and PII from being released.

While RMS360 was meant to be the default data extraction tool since 2010, functionally the Clearinghouse used both EPIR and RMS360 depending on the data request. Since April 2019, as a result of the Clearinghouse breach, employees have been instructed to use EPIR exclusively because it defaults to not releasing 6(b) information and PII.

A number of individuals interviewed stated that part of the reason that the restricted information was disclosed was that each RMS360 report, potentially

containing thousands of data lines, had to be manually reviewed. Further, interviewees also noted that potentially redactable information was not always found in the same column, thus making manual reviews both more challenging and time-consuming. Several individuals stated that if the data were initially scrubbed and then published online, like the NEISS database, then the public could search for the information independently, and there would be fewer data requests for Clearinghouse staff to fulfill, thus fewer opportunities to release restricted information.

Section 6(b) Requirements

The CPSC is generally required to prevent public disclosure of information which can identify a manufacturer or a private labeler of products.[23] The CPSC can only release information which can tie a type of product to a specific manufacturer or private labeler with advance notice of more than 15 days unless there is a finding that public health and safety require a shorter notice period.[24] Section 6(b) prohibits the CPSC from disclosing Clearinghouse information without taking reasonable steps to ensure that the information is accurate, that disclosure of the information is fair under the circumstances, and that disclosure of the information is reasonably related to effectuating the purposes of the CPSA and of the other laws administered by the Commission. Section 6(b) requirements are meant to incentivize manufacturers to provide the maximum possible amount of safety information while minimizing the chance that a manufacturer or private labeler will be injured by the release of inaccurate information about its product.

Personally Identifiable Information

PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Examples of PII include: names of individuals (unless they have consented to release); personal addresses or telephone numbers; driver's license numbers; social security numbers; passport numbers; bank account information; credit card information; medical reports; and biometrics. The following can be considered PII when combined with other PII: date of birth, date of death, age, sex/gender, or race.

[23] 15 U.S.C. § 2052(a)(12) defines a "private labeler" as an owner of a brand or trademark appearing on the label of a consumer product other than the manufacturer of the product.
[24] 16 CFR 1101.21-1101.26.

The OIG found:

10. The CPSC maintains multiple data extraction tools because no one tool fully meets the agency's needs. The first has limited search capability but more adequately protects 6(b) information and PII data. The second is defaulted to release restricted information but has more search capabilities. The third tool is rarely used because most staff have not been trained in its use.
11. Clearinghouse staff were unable to provide evidence of the existence of implemented policies and procedures related to responding to data requests, use of data extraction tools, or requirements and methodologies to protect 6(b) information and PII data.
12. Manually reviewing the responses to data requests, which can include thousands of rows of information, leads to an unreasonably high risk of restricted information being released to the requestor.

The OIG recommends CPSC management:

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.
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.
19. Limit access to the underlying database and the data extraction tool to those with a bona fide need for access.
20. Create a searchable online public database with scrubbed Clearinghouse data to reduce the number of individual Clearinghouse information requests that are processed.

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.
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.
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.
24. Require additional training for Clearinghouse supervisory staff, up to and including the AED for EPHA, on effective review of Clearinghouse staff output.
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.
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.
27. Require supervisory review of all completed Clearinghouse data requests.
28. Use the data from the tracking system to develop and publish annual statistics related to the work of the Clearinghouse.
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.
30. Enforce Principle of Least Privilege and limit access to data on the P-drive to individuals with a bona fide “need to know.”

Internal Control

Agency managers are responsible for designing and implementing appropriate internal controls for the programs over which they have authority. These responsibilities flow primarily from the FMFIA which requires managers to provide assurances that funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation. Managers are required to sign an annual statement of assurance stating that the systems of internal accounting and administrative control under their management fully comply with FMFIA requirements. OMB Circular A-123 (A-123), *Management's Responsibility for Enterprise Risk Management and Internal Control*, which is the implementing guidance for the FMFIA, states:

> Internal control is an integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved: effectiveness and efficiency of operations . . . and compliance with applicable laws and regulations.

The GAO's Green Book sets internal control standards for federal entities. According to the Green Book, internal control helps an entity:

- manage its operations efficiently and effectively
- report reliable information about its operations
- comply with applicable laws and regulations

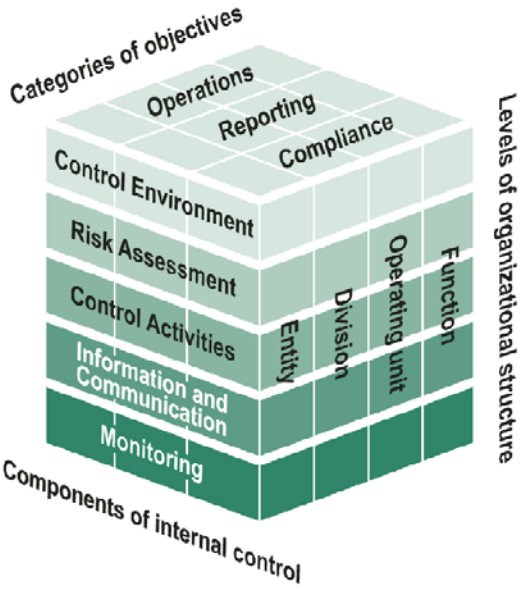
Internal control, in the broadest sense, is the process used by management to help it achieve its objectives and includes processes for planning, organizing, directing, controlling, and reporting on agency operations.

Common examples of internal controls include: supervisory review of a subordinate's work product, segregation of duties, reconciliations of accounts, annual inventories, drafting and implementing standard operating procedures, tracking program outputs, regularly reviewing the results of the tracking, and providing training to employees to ensure they understand the policies and procedures relevant to their duties.

Management is responsible for the design, implementation, and operation of an effective internal control system. As part of this responsibility, management sets the entity's objectives, implements controls, and evaluates the internal control system. However, individual employees throughout the entity play important roles in implementing and operating an effective internal control system. An effective internal control system increases the likelihood that an entity will achieve its

objectives. Conversely, the lack of an effective internal control system decreases the likelihood that an entity will achieve its objectives. In regard to the Clearinghouse, management neither designed nor implemented an effective internal control system.[25]

The standards in the Green Book are organized by the five components of internal control. Each of the five components of internal control contains several principles. Principles are the requirements of each component. The five components apply to staff at all organizational levels and to all categories of objectives as shown below.



Sources: COSO and GAO. I GAO-14-704G

CPSC management had an obligation under FMFIA, A-123, and the Green Book to design, implement, and operate internal controls over the Clearinghouse. The OIG will use the Green Book's five component paradigm to assess CPSC's internal controls over the Clearinghouse.

Control Environment

This is the foundation for an internal control system. It provides the discipline and structure to help an entity achieve its objectives. It consists of the following principles:

[25] There were certain agency wide internal controls in place that covered aspects of the Clearinghouse Program, such as the requirement that employees use the WebTA application to record their hours worked, leave taken, etc. However, no internal controls specific to the Clearinghouse Program were found. Even in regard to the tracking of hours worked, no efforts were made to track the number of hours any individual employee worked on tasks related to answering Clearinghouse data requests, only on the total number of hours they recorded in any given pay period.

	Internal Control Principles	Present in the Clearinghouse
Control Environment	1. Demonstrate commitment to integrity and ethical values	No
	2. Oversee the internal control system	No
	3. Establish organizational structure, assign responsibility, and delegate authority to achieve objectives	No
	4. Demonstrate commitment to a competent workforce	No
	5. Evaluate performance and hold people accountable for their internal control responsibilities	No

1. Demonstrate commitment to integrity and ethical values

The first task of management is to set a tone at the top demonstrating the importance of integrity and ethical values and communicating these values throughout the organization. This broad mandate should then be supported by a working internal control system and a structure to enable CPSC staff to meet objectives regarding operations, reporting, and compliance.

There is no evidence that EXHR management made any substantive effort to demonstrate a commitment to integrity and ethical values or to communicate these values throughout the Clearinghouse. In fact, there is evidence that agency management routinely demonstrated at best a reckless disregard for the truth and at least one example of a deliberate fabrication.

The OIG found numerous examples of problems regarding integrity and ethical values in the Clearinghouse.[26] These problems involved both systemic issues and

[26] One such example occurred when the AED for EXHR was asked to provide copies of the up-to-date PII inventories relied upon in assessing the status of internal controls in the relevant offices. The OIG was initially provided a link to the CPSC's System of Records Notices and informed that some were used for "checks on PII inventories." When asked to explain the relevance of the System of Records Notices to PII inventories and what "checks on PII inventories" are, the AED for EXHR admitted that none of the offices in question had PII inventories.

The AED for EXHR stated that he and his subordinates referenced PII inventories in their statements of assurance and claimed that they were up to date because, "The template for the letters of assurance contained a statement that the Office[']s Personally Identifiable Information (PII) inventory is up to date." He offered no explanation as to why he and his subordinates thought it appropriate to take a statement out of a template that was not true and place it in actual statements of assurance; nor was any reassurance offered that other untrue statements had not been included in the relevant statements of assurance for similar reasons.

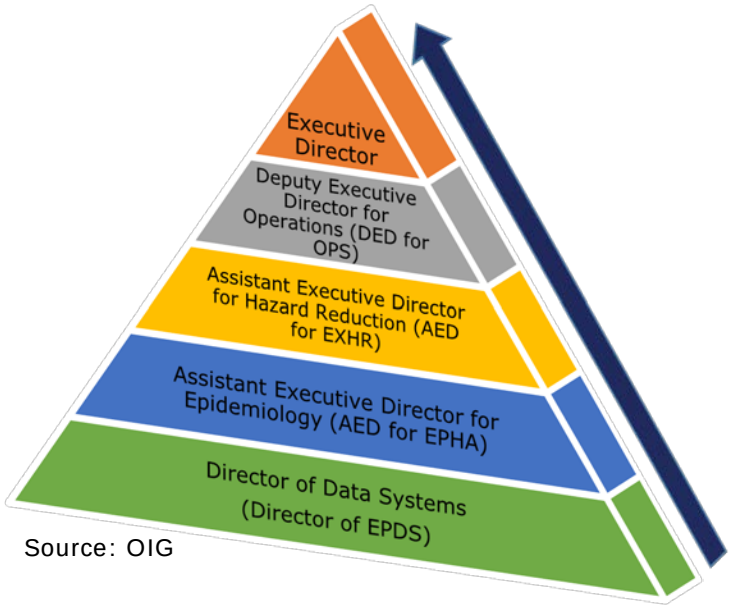
He then went on to explain that, "We do not have a PII inventory, but to provide reasonable assurance for this statement we reviewed the following systems that may contain PII . . ." No effort was made

examples of individual managers failing to uphold government standards regarding integrity or ethical values.

The most egregious example of a systemic ongoing failure by agency management to demonstrate a commitment to integrity and ethical values involved the statements of assurance relevant to the Clearinghouse. Agency officials were grossly negligent at best and lied at worst when they signed statements of assurance indicating that internal controls regarding the Clearinghouse were in place and operating effectively.

Annually, offices are required to review their internal controls and provide management with a statement of assurance that internal controls in the area under their supervision are in place and functioning in such a way as to provide assurance that management's objectives are met. The process should roll up through the organization with each successive layer of management agreeing with their subordinate's assessment and accepting the statement of assurance or questioning the accuracy of the report.

The pyramid below is the OIG's representation of EXHR's statement of assurance hierarchy:



Source: OIG

to explain how not having a PII inventory and reviewing systems that may contain PII would create a reasonable assurance that an office had an up-to-date PII inventory. Further, the notion that EXHR and its subsidiary offices had done anything related to PII inventories was greatly undercut by reports from EXIT and OGC that, contemporaneously to EXHR's email exchange with the OIG on this point, EXHR staff were contacting EXIT and OGC and requesting the definition of the term "PII inventory."

The content of these statements of assurance are relied upon by the CPSC's Executive Director when she makes her statement of assurance to the Chairman, and by the Chairman when signing an annual consolidated statement of assurance for the agency as a whole. These consolidated statements of assurance were presented to and relied upon by independent auditors, OMB, Congress, and the American people. In the event of problems with internal controls, each level of management up to and including the Chairman has the option to sign a statement of assurance which includes a specific disclaimer related to a portion of agency operations.

The Chairman's consolidated statements of assurance for 2014 through 2018 do not contain any disclaimers. However, several of the managers responsible for either providing input to or preparing statements of assurance covering the Clearinghouse indicated in interviews with investigators from this office that they had been aware for years of problems with the internal controls governing the Clearinghouse. Despite being aware of these problems, they did not note them in their statements of assurance.[27]

Specifically, in the statements of assurance for 2017 and 2018, the former AED for EXHR, the Deputy AED for EXHR, the AED for EPHA, and the Director of EPDS all issued statements of assurance indicating that there were no problems with internal controls regarding the Clearinghouse.

And for FY 2019, the acting AED for EXHR issued a statement of assurance on September 9, 2019, approximately five months after the agency was made aware of the data breach, that indicated:

- programs in his division, which includes the Clearinghouse, achieved their intended results
- laws and regulations were followed
- effective monitoring processes were maintained to assess internal controls
- there were no material weaknesses in the design and operation of management controls

This was the acting AED for EXHR's assessment of internal controls after agency management learned that the largest data breach of 6(b) information and PII in the history of the CPSC had occurred.

[27] The former AED for EXHR, AED for EPHA, Director of EPDS, and Supervisory Program Analyst.

As part of the 2019 Financial Statement Audit, this office questioned the validity of EXHR's statement of assurance. This statement of assurance was drafted by the current AED for EXHR in his capacity as the acting AED for EXHR. The CPSC subsequently retracted the FY 2019 EXHR Statement of Assurance and a second statement of assurance was issued. This second statement of assurance acknowledged that "insufficient design and operation of internal controls" had resulted in a data breach which had in turn led to the improper disclosure of 6(b) information and PII.

One of the critical elements in this data breach was the disclosure of PII. Federal regulations and best practices require organizations which control PII to maintain an up-to-date inventory of PII as a basic control over PII.[28] In the years preceding the data breach, a number of the supervisors involved in the data breach issued statements of assurance claiming that their organizations had up-to-date PII inventories. This was surprising given that in past FISMA reviews the CPSC had acknowledged that it did not maintain PII inventories. In light of the above, the OIG asked the Director of EPDS, the current AED for EXHR, and the AED for EPHA, for copies of the PII inventories that they claimed to have and claimed to rely on in making their statements of assurance: none were provided. Ultimately, the current AED for EXHR acknowledged that they never had PII inventories, up to date or otherwise. (See footnote 26 in the section "Control Environment" for additional details.)

2. Oversee the internal control system

Throughout the EPHA supervisory chain there was an awareness of problems in the Clearinghouse. Numerous supervisors interviewed as part of this investigation[29] indicated they had been aware of internal control problems[30] regarding the Clearinghouse.[31] Somehow, these supervisors failed to internalize the fact that their duties included ensuring that there were adequate internal controls over the program or, at a minimum, making senior agency management, such as the Executive Director or Chairman of the CPSC, aware of the internal control deficiencies.

[28] Including but not limited to the following: OMB Circular A-130, National Institute of Standards and Technology Special Publication 800-122, National Institute of Standards and Technology Special Publication 800-53, revision 4.
[29] The former AED for EXHR, AED for EPHA, Director of EPDS, and Supervisory Program Analyst.
[30] Although none of the supervisors used the phrase "internal control" the problems they described: lack of supervisory review, failure to provide training, lack of written policies and procedures, etc. all relate to problems with internal controls.
[31] A number of supervisors also raised concerns about staffing levels. However, there is no indication that additional staffing would have in any way addressed the failures of internal control that led to the data breach.

The problems with internal control regarding the Clearinghouse appear to have started at the top of EXHR and permeated downward to include all levels of supervision as well as line employees. The former AED for EXHR indicated a lack of appreciation for the work done through the Clearinghouse and a lack of understanding of the accompanying risks if that work was not carried out properly. Specifically, in an interview with the OIG, he stated that after being asked by the Office of the Executive Director to determine what had been improperly released to Consumer Reports, he ". . . became acquainted with the tracking spreadsheet." Compounding the fact that he did not know about this internal control until after the data breach had occurred, staff indicated that they did not always use the tracking spreadsheet to record completed work.

In fact, the tracking spreadsheet proved to be so unreliable that when the time came to determine the size and scope of the data breach, the CPSC found it could not rely on it. The agency fell back on reviewing the copies of outgoing emails sent to the Clearinghouse mail box as instructed. Again, agency staff realized they had not identified all potential breaches. Finally, they judgmentally sampled a population of over 14,000 emails based on items discovered in their earlier reviews.

Furthermore, even lower level supervisors were aware of their senior manager's lack of interest in the Clearinghouse. In his interview with the OIG, the Director of EPDS stated that, "EXHR management has never even been down in EPDS to see what is done on a day to day bases [*sic*]."

3. Establish organizational structure, assign responsibility, and delegate authority to achieve objectives

Numerous witnesses acknowledged management's failure to implement written policies and procedures or hold formal training regarding the release of information through the Clearinghouse program. These statements are supported by the lack of formal written policies, procedures, and other job aids such as checklists, manuals, and automated workflows.

This problem was compounded by the failure to formally establish structures, reporting lines, authorities, and responsibilities. Perhaps even more telling, there weren't even policies or procedures requiring supervisors to review Clearinghouse work performed by line employees.

4. Demonstrate commitment to a competent workforce

Far from demonstrating a commitment to a competent workforce in the Clearinghouse, management failed to provide training or adequately supervise the work performed by its workforce. This near total lack of implemented internal controls includes the lack of formal training regarding both the use of the tools to

complete their work and the importance of recognizing and redacting 6(b) information and PII. Staff was instead left to rely on their recollections of whatever informal on-the-job-training they had received when they started working at the CPSC.

As one program analyst stated:

> I was not trained using a document outlining standard procedure and I never received any reference document for future use. I was personally walked through how to use [*RMS*]360, EPIR and SAS with no written information.

A second program analyst stated:

> . . . there has been no formal [*RMS*]360 training (in general or specific to researching requests with the exception of to put in the date range of the search, the appropriate product codes and manufacturer if that was requested), there was no formal sit down training from [*redacted*] regarding information request processing.

Similarly, employees did not have a clear recollection of whether or not they had received training on safeguarding 6(b) information, as shown by these statements from two Clearinghouse employees:

> Employee #1: To the best of my knowledge, there was no training on 6(b) and its relative importance to the work I was doing.
>
> Employee #2: I am not specifically familiar with 6(b). If I had received training, it may have been 5-6 years ago.

5. Evaluate performance and hold people accountable for their internal control responsibilities

The CPSC failed to hold Clearinghouse management accountable for the safe and effective operation of the program prior to the breach. None of the performance evaluations the OIG reviewed had any Clearinghouse specific performance metrics. After the data breach and the initiation of investigations by the Senate Commerce Committee and this office, the CPSC did take these events, including the failures of internal control leading up to the data breach, into account in the performance appraisals of four of its employees.

Risk Assessment

This allows management to assess the risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses. It consists of the following principles:

	Internal Control Principles	Present in the Clearinghouse
Risk Assessment	6. Identify risks and define risk tolerances	No
	7. Identify and analyze risk in relation to objectives	No
	8. Evaluate fraud risks	No
	9. Identify and analyze changes that could significantly affect internal controls	No

6. Identify risks and define risk tolerances
No evidence was found that a formal or informal risk assessment process was ever designed, performed, or implemented.

7. Identify and analyze risk in relation to objectives
Neither the supervisors nor the line employees interviewed were able to identify formal risks or objectives related to the Clearinghouse Program.[32]

8. Evaluate fraud risks
No risk assessment of any type was completed. There is no indication that agency management ever attempted to identify and evaluate fraud risks related to Clearinghouse activities.

9. Identify and analyze changes that could significantly affect internal controls
No risk assessment was completed. There is no indication management identified and analyzed changes that could significantly affect internal controls.

Control Activities

These are the actions management takes through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the entity's information system. It consists of the following principles:

[32] Several interviewees mentioned "soft" aspirational timelines but no witness was able to identify any written criteria.

	Internal Control Principles	Present in the Clearinghouse
Control Activities	10. Design control activities to achieve objectives	No
	11. Design and implement information system controls	No
	12. Implement control activities through policies	No

10. Design control activities to achieve objectives

The OIG found no evidence of the existence or design of any:

- implemented policies and procedures to govern the processing of requests for information[33]
- formal training program for employees with duties related to the Clearinghouse
- checklists to aid employees in carrying out their reviews of requests for information
- indication that supervisory review of the work performed by line employees was either required or regularly took place

11. Design and implement information system controls

The lack of adequately designed and implemented control activities or information technology controls played a role in both the inadvertent disclosures of information to external parties that led to this investigation and to the potential inadvertent disclosures of information to parties without a "need to know" the information within the CPSC.

As discussed in greater detail in the section "Data Sources and Extraction Tools," in 2010, management recognized the weaknesses of EPIR and commissioned RMS360 to address those weaknesses. While RMS360 did address some of the weaknesses associated with EPIR, RMS360 introduced new weaknesses. The most relevant of which was that RMS360 defaulted to releasing 6(b) information and PII. Management accepted delivery and authorized the operation of RMS360 with these shortcomings along with 65 other known security weaknesses.[34] The fact that they

[33] A number of interviewees referred to the existence of an SOP developed by a former CPSC employee. Most of the interviewees had never heard of this SOP. The interviewees who had heard of it largely reported that they did not have a copy of it or access to a copy of it. No copy of the SOP was available on the CPSC's intranet site. When a copy of this SOP was finally found, it was determined that although it did deal with the extraction of information using one of the relevant IT systems, it did not contain guidance related to the handling of 6(b) information or PII or its release. Additionally, given employees' lack of knowledge of its existence and the difficulty surrounding finding a copy of it, the SOP in question was clearly not implemented.

[34] The CPSC's own annual CPSRMS Security Assessment Report identified 65 controls that were "Other-Than-Satisfied."

did not turn off the old tool, EPIR, reflects some level of awareness that the new tool had serious flaws. Additionally, management should have been cognizant of the inefficiencies inherent in expending resources to support two tools instead of one.

However, while CPSC management should have been aware of these failings it still allowed RMS360 to be deployed and made no apparent move to correct or eliminate these failings.

In addition to the data breach related to the inadvertent release of 6(b) information and PII to entities "outside" of the CPSC (such as Consumer Reports) through the Clearinghouse, evidence was found that the CPSC also failed to design or implement adequate automated technology controls to enforce the "Principle of Least Privilege." This resulted in a failure to secure 6(b) information and PII from unauthorized releases within the CPSC to employees who had no "authorized purpose" to justify their access to the information in question. The CPSC lacks adequate internal controls over its intranet to allow us to determine how many individuals with no authorized purpose actually accessed the PII on the P-drive. The OMB's definition of "breach" includes situations in which unauthorized users have access or potential access to PII.[35] Thus, this failure to secure information internally contributes to the scope of the data breach.

As explained by the AED for EPHA:

> PII or 6(b) data is not masked internally. Anyone who can access the P-drive where the source documents are held (or the applications/DBs [*data bases*] hosting the data) can see all the data unmasked.
>
> Source death certificates, medical examiner reports, and IDI information are maintained on the P-Drive.

And as noted by the Director of EPDS:

> Everybody in the agency can pull data from [*RMS*]360 . . . not just the Clearinghouse. We can't see when others pull data. Also, they can get to the source documents either through the data pull in EPIR or [*RMS*]360 or going straight to the P: drive. Why do people need access to Death Certificates and unredacted source documents on the P: drive?

[35] See OMB M 17-12

During a recent IT security assessment, the OIG determined that at least 355 individuals at the CPSC had access to the P-drive and the PII and 6(b) protected data it contained. This far exceeds the number of CPSC employees with any "need to know" the information in question. A recent review of the contents of the P-drive indicated that in addition to Clearinghouse data it may also contain other PII, such as employees' signatures and copies of IDI reports.

In addition to a lack of control over access to the data, the Clearinghouse staff also lacked automated processes to assist in the managing of requests for information. There was no automated workflow, automated supervisory review, or automated tracking of receipt and fulfillment of Clearinghouse data requests.

12. Implement control activities through policies

Clearinghouse management relied on unwritten policies to manage Clearinghouse activities. For example, a process did exist that was supposed to allow for tracking information requests made to the Clearinghouse. This process involved having Clearinghouse employees send a courtesy copy (cc) to an organizational email box each time they responded by email to a request for information. There is no evidence that management ever actually documented, implemented, or enforced this requirement. As a result, several interviewees indicated that this process was not consistently followed. The lack of documented control activity policies extended to all facets of the Clearinghouse's activities as discussed throughout this report.

In conclusion, EXHR aggravated its lack of documented policies and procedures regarding the Clearinghouse Program with a lack of formal training for employees with responsibilities related to the Clearinghouse Program. The above problems were then compounded by a lack of supervisory review. In addition to not training their employees adequately to do their jobs correctly, they failed to monitor their performance. The results of the above failures are illustrated in the following statement from a program analyst:

> To the best of my knowledge, there was/is no documentation on what to redact for the Clearinghouse requests. I understood from verbal instructions that retailer reports (records that start with a Y or are from Sections15b[*sic*]), addresses, manufacturer, and model information should generally be deleted. The first erroneous file I sent out for a Clearinghouse request was [*redacted*] on October 16, 2018. The file name is Fire Pits.xlsx[.] I sent the file to [*redacted*] to review for errors before sending out. It went out with both model and manufacturer information and a long narrative all of which are not supposed to be released. We both missed it. This has been happening since 2013.

Information and Communication

This supports internal control by providing internal and external stakeholders timely, reliable, and relevant information. It consists of the following principles:

	Internal Control Principles	Present in the Clearinghouse
Information and Communication	13. Incorporate quality information throughout the internal control process to achieve the program's objectives	No
	14. Communicate quality information internally	No
	15. Communicate quality information externally	No

13. Incorporate quality information throughout the internal control process to achieve the program's objectives

There was no discernable collection of relevant information to be used in support of the Clearinghouse; there was no timekeeping system to track staff resources used for Clearinghouse activities; and there was no effective system to track requests made and fulfilled.

The AED for EPHA acknowledged that there was:

> . . . no automated workflow for information requests to systematically require supervisory review of information requests. A mailbox ("Clearinghouse") exists that the rep answering the request is asked to CC [*sic*], but if the rep makes an error and does not CC [*sic*] the Clearinghouse email group, there is nothing to catch it.

He also acknowledged that:

> The tracking was imperfect. No automated solution has been implemented to address the tracking issue where employees were supposed to copy the Clearinghouse email when responding to requests.

14. Communicate quality information internally

Because no performance information was captured, management lacked quality information necessary to effectively manage the Clearinghouse.

15. Communicate quality information externally

Statements of assurance are the primary means by which accurate information regarding both the status of internal controls and whether or not the Clearinghouse is meeting its objectives should have been communicated both to agency senior management as well as to external stakeholders such as OMB, Congress, and the American people.

Because no performance information was captured, management had no accurate performance data to report externally regarding the Clearinghouse. Similarly, they had no basis to opine on the effectiveness of internal controls.

As discussed above in the section, "Demonstrate Commitment to Integrity and Ethical Values," (see p. 34, in the section "Control Environment") for additional details the statements of assurance prepared by those responsible for the management of the Clearinghouse were, at best, inaccurate; and at worst, contained deliberate fabrications.

For example, as previously discussed, the statements of assurance issued for FY 2017 by the Director of EPDS, the former AED for EXHR, and AED for EPHA, as well as the statement of assurance issued for FY 2018 by the AED for EPHA all indicated that the relevant offices each had an up-to-date PII inventory. Management was unable to provide copies of PII inventories. Ultimately, the current AED for EXHR acknowledged that they did not actually have PII inventories, up to date or otherwise.

The breakdown in external communications regarding the Clearinghouse Program extends beyond internal controls and statements of assurance. Indeed, it appears that the breakdown involves both a lack of effective internal controls, including monitoring processes, and also a lack of management interest in accurate measurement of program outcomes.

A stark example of this near total lack of control/awareness of the information relevant to both internal control throughout the system and information relevant to the Clearinghouse is the orphaned Epidemiology webpage.[36] It contains references to the National Injury Information Clearinghouse, its functions, and that it answered 4,000 information requests per year. When the OIG was unable to validate these numbers, the OIG inquired of agency management the source of the numbers and the individuals responsible for posting/updating them. No management official was willing to take responsibility for or able to explain the

[36] https://www.cpsc.gov/epidemiology/cpsc_epi/clearinghouse.html At the time of this investigation this webpage is still accessible via Internet search engine, but is no longer directly linked to the CPSC website.

source, relevance, or accuracy of the information posted on the orphaned Epidemiology webpage regarding the Clearinghouse.

The Director of EPDS stated, "I do not know where the 4,000 annual requests come from that is found on the CPSC website and who comes up with that number. Maybe it was 4,000 including FOIA and OCM requests."

Indeed, no one that we interviewed was able to identify either the source of the information on the public facing webpage or the office/individual who would be responsible for providing such information to the public.

Monitoring

This is the dynamic process where management assesses the quality of performance over time and promptly resolves the findings of audits and other reviews. It consists of the following principles:

	Internal Control Components	Present in the Clearinghouse
Monitoring	16. Monitor the internal control system and evaluate the results	No
	17. Remediate identified internal control deficiencies on a timely basis	No

16. Monitor the internal control system and evaluate the results
There was no monitoring because management did not perform any of the other internal control activities.

17. Remediate identified internal control deficiencies on a timely basis
As discussed earlier in the section "Prior Audit Results and Unaddressed Recommendations," management has been on notice since 2010 about weaknesses regarding Clearinghouse operations and IT security concerns. Over the years, the OIG has made six recommendations relevant to the Clearinghouse. While management addressed one of the six recommendations, recommendations related to data encryption/security and training remain open. In addition, since accepting delivery in 2010, management failed to address the 65 known security weaknesses inherent in RMS360. When asked about implementing OIG recommendations, the Director of EPDS stated, "I never saw the IG [*Inspector General*] report . . . Nobody ever discussed closing out recommendations or fixing the issues."

The OIG found:

13. Management neither designed nor implemented Clearinghouse internal controls adequate to meet any of the seventeen principles associated with the five components of internal control. The CPSC relied on and reported incomplete and inaccurate data and did not perform adequate due diligence and oversight of the work of Clearinghouse staff in reporting breach statistics.

The OIG recommends CPSC management:

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.
32. Determine, document, and implement a structure for the Clearinghouse.
33. Determine, document, and implement the role of the Freedom of Information Act Office in responding to Clearinghouse requests.
34. Require the Office of Human Resources Management (Human Resources) to provide consultation to ensure that the organizational structure in EPDSI 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.
35. Implement the recommendations from the Human Resources study.
36. Complete and document the results of a risk assessment of Clearinghouse operations.
37. Design, document, and implement control activities to respond to the results of the completed risk assessment process.

38. Develop and implement written guidance on the importance of the statements of assurance process and the related documentation requirements.
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.
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.

Conclusion

The OIG was tasked with the following:

- Determine the scope and root causes of the Clearinghouse data breach
- Investigate allegations that:
    - there was collusion between CPSC employees and employees of Consumer Reports
    - the data breach was deliberate
    - certain CPSC employees made threats against both Consumer Reports and CPSC employees
- Assess the CPSC response to the data breach including whether the response was compromised by utilizing CPSC employees who were responsible for the breach in key roles in the breach response

The OIG determined that the scope of the data breach greatly exceeded the agency's estimate. The data breach lasted from at least 2010 to 2019, rather than 2017 to 2019 as the agency publicly stated. Similarly, the OIG determined that in addition to the external data breach, involving inadvertent disclosures of information to external requestors, there was an internal data breach. The internal data breach involved CPSC employees having access to confidential information they did not have a "need to know."

The OIG determined that the root causes of the data breach were mismanagement and incompetence. The mismanagement was primarily manifested in the lack of effective internal controls over the Clearinghouse and EXHR management's lack of integrity regarding this lack of internal controls. The incompetence manifested in the lack of supervision, documented policies and procedures, and training for nonsupervisory and first level supervisory Clearinghouse employees.

There were multiple material weaknesses in the system of internal control over the Clearinghouse. In fact, none of the Green Book's 17 principles of internal control were in place. This absence of internal controls coupled with a lack of integrity regarding the reporting of the effectiveness of internal controls allowed the Clearinghouse to operate without:

- effective oversight
- a functioning organizational structure
- performance measurement
- defined goals
- risk assessments

- controls designed to mitigate risks
- effective IT system controls
- policies and procedures for the work of the Clearinghouse
- quality programmatic information reported internally and externally
- ongoing program monitoring
- implementation of prior audit recommendations

The OIG concludes there is no evidence that there was collusion between the CPSC and Consumer Reports or that the breach was deliberate. The OIG concludes there is no evidence that staff at CPSC or Consumer Reports were threatened by CPSC staff.

The OIG concludes there were significant deficiencies in the CPSC's response to the data breach. After becoming aware that a data breach had occurred, the CPSC attempted to keep Congress and other stakeholders informed regarding the CPSC's response to the data breach. This effort was hobbled by the CPSC's lack of preparation for crisis management. Further, the CPSC's response to the breach was compromised by utilizing CPSC employees who were responsible for the breach in key roles in the breach response. This resulted in an under estimation of the scope of the data breach. This failure to properly grasp the scope of the data breach resulted in inaccurate information being reported to Congress and the American people. It also resulted in inaccurate estimates being used by the BRT and senior agency management in their attempts to determine how to respond to the data breach. The CPSC now needs to conduct a new assessment of the scope of the data breach and its impact. After conducting this assessment, the CPSC should determine what corrective actions are appropriate to address the cause(s) of the data breach and its consequences. Finally, the CPSC needs to take corrective actions to address the findings in this report and improve internal controls regarding the Clearinghouse.

The results of this investigation should assist the CPSC in identifying and prioritizing remedial efforts to improve the agency's security posture to prevent future data breaches, determine the scope of the breach, and assess what additional corrective actions should be taken by the agency.

We provide 40 actionable recommendations. When completed, these recommendations should significantly improve the Clearinghouse's management and operations.

APPENDIX A: Full Chronology

2014-2018:

- Consolidated statements of assurance signed by the Chairman did not contain any disclaimers, despite employees knowing of internal control problems.

2017-2018:

- In the statements of assurance for 2017 and 2018, the former AED for EXHR, the Deputy AED for EXHR, the AED for EPHA, and the Director of EPDS all issued statements of assurance indicating that there were no problems with internal controls regarding the Clearinghouse.

March 31, 2019:

- Consumer Reports requested a phone call with the acting Director of Communications and the Executive Director to discuss data CPSC had sent them.

April 1, 2019:

- The Executive Director asked the acting Director of Communications to contact Consumer Reports.
- Consumer Reports notified the CPSC that it had received data from CPSC staff that included manufacturer-specific material which should have been redacted.
- CPSC staff requested that Consumer Reports return the data and destroy any copies; Consumer Reports refused.
- The Executive Director asked the DED for OPS to look at the nature of the Consumer Reports data request and what was actually sent.
- In turn, the DED for OPS consulted the individual responsible for the Clearinghouse group, the AED for EPHA, who had his team look into the scope of the problem and if it was limited to just Consumer Reports.
- The AED for EPHA became “acquainted” with the Clearinghouse operations and how data requests were tracked.
- The former AED for EXHR learned of the unauthorized disclosure at 5:30 pm.
- The former AED for EXHR contacted the Director of Product Safety at Consumer Reports that evening and asked him not to release the information.
- The Director of Product Safety at Consumer Reports stated that the matter was with the Consumer Reports Office of General Counsel and out of his hands.

April 2, 2019:

- An attorney from the CPSC Office of General Counsel Enforcement and Information Division was notified of the breach.

April 3, 2019:

- An Associate General Counsel at Consumer Reports received a letter from the CPSC Office of General Counsel stating "this information cannot be published or further disseminated by Consumer Reports." Consumer Reports refused to return or destroy the information it had received.

April 5, 2019:

- CPSC senior management asked the AED for EPHA to provide a full count of all data breaches by April 10, 2019.
- The SAOP was notified of the breach and began to determine whether to call together the BRT.

April 10, 2019:

- AED for EPHA reported that between December 2017 and March 22, 2019, the Clearinghouse made improper disclosures to 29 unique entities. The bulk of the disclosures went to two entities: Consumer Reports and a researcher at a state university. These disclosures contained information on approximately 10,900 unique manufacturers, as well as street addresses, ages, and genders of approximately 30,000 consumers.
- The AED for EPHA reported to senior leaders that there was one disclosure before 2017; an email sent in 2013 whose intended recipient was allegedly a CPSC employee, but it was inadvertently sent to a similarly-named manufacturer employee.

April 11, 2019:

- CPSC staff began sending notifications to the 10,900 manufacturers identified in the disclosures. This process involved five phases of correspondence with affected manufacturers.

April 15, 2019:

- The SAOP determined that the BRT needed to be formed to deal with the unauthorized disclosure of PII.

April 16, 2019:

- The BRT met.

April 26 to May 23, 2019:

- AED for EPHA asked EXIT to pull all emails with attachments sent out by Clearinghouse employees.
- The emails were pulled in 19 separate tranches.

May 6, 2019:

- Consumer Reports was notified that they had received PII in the information released in the unauthorized disclosure.

May 7, 2019:

- The BRT presented a memorandum containing its findings to the former Acting Chairman who accepted the recommendations and signed the memo.

May 9, 2019:

- Consumer Reports certified destruction of the PII it received from CPSC.

June 14, 2019:

- Former AED for EXHR leaves the agency. Deputy AED for EXHR named as acting AED for EXHR.

July 31, 2019:

- All recipients of unauthorized disclosures have agreed to return or destroy the information contained in the disclosures except for Consumer Reports who kept the 6(b) information and used it.

September 9, 2019:

- The acting AED for EXHR issued a statement of assurance that indicated programs in his division (including the Clearinghouse) achieved their intended results; laws and regulations were followed; effective monitoring processes were maintained to assess internal control; there were no material weaknesses in the design and operation of management controls. This was five months after the data breach.

September 18, 2019:

- The acting AED for EXHR is selected as the current AED for EXHR.

September-November 2019:

- The validity of EXHR's 2019 Statement of Assurance was questioned by the OIG as part of the 2019 Financial Statement Audit. The CPSC subsequently retracted it and a second statement of assurance was issued on November 18, 2019.

APPENDIX B: Summary of Internal Control Findings

Internal Control Component	**Principles** (edited for length)	Summary of Findings
Control Environment	1. Demonstrate commitment to integrity and ethical values 2. Oversee the internal control system 3. Establish organizational structure, assign responsibility, and delegate authority to achieve objectives 4. Demonstrate commitment to a competent workforce 5. Evaluate performance and hold people accountable for their internal control responsibilities	• statements of assurance indicated that there were no problems with internal controls despite managers being aware of problems • deceptive/false official statements were made regarding the scope of the inadvertent disclosures • management did not have a great appreciation for Clearinghouse operations • Clearinghouse management did not appreciate the dangers of releasing 6(b) information. • no supervisory review of work performed • no formal training only "some" on-the-job training when staff were first hired • no implemented policies and procedures • no active supervision • no demonstrable commitment to hold people accountable prior to data breach
Risk Assessment	1. Identify risks and define risk tolerances 2. Identify and analyze risk in relation to objectives 3. Evaluate fraud risks 4. Identify and analyze changes that could significantly affect internal controls	• no formal standards or objectives • no risk assessment • no fraud risk assessment • no internal controls much less any analysis of same
Control Activities	1. Design control activities to achieve objectives	• no control activities identified (no formal training, no checklist to aid review, no supervisory review, no training program, etc.)

	2. Design and implement information system controls 3. Implement control activities through policies	• no automated processes • problems with information system controls • no implemented policies and procedures
Information and Communication	1. Incorporate quality information throughout the internal control process to achieve the program's objective. 2. Communicate quality information internally 3. Communicate quality information externally	• no discernable collection of relevant information • no one able to explain the relevance or accuracy of the information posted on the orphaned Epidemiology webpage re: Clearinghouse. • two methodologies developed to track work, neither used consistently
Monitoring	1. Monitor the internal control system and evaluate the results 2. Remediate identified internal control deficiencies on a timely basis	• no internal controls implemented • no effort by management to acknowledge and monitor internal control deficiencies • consistently reported "no problems" with internal controls • no effort to correct internal control deficiencies raised by prior audits

APPENDIX C: Consolidated List of Recommendations

1. Reconvene the BRT to assess the full extent of the breach, and base its response on the totality of the breach.
2. Establish blanket purchase agreements for identity monitoring, credit monitoring, and other related services for data breach victims.
3. Complete and publish a document describing lessons learned after the BRT completes its work related to this 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.
5. Conduct an annual Breach Response Policy plan review.
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.
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.
8. The crisis communication plan should include annual tabletop exercises and annual plan reviews.
9. The CPSC should document the results of each crisis communication plan annual tabletop exercise.
10. The CPSC should publish the resulting comprehensive crisis communication plan after any update.
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.
12. Review all available data and establish an accurate identification of all data inadvertently released, internally and externally, from 2010 to 2019.
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.
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.
15. Establish a process for communicating and enforcing the implementation of recommendations previously agreed to by management, as required by law.

16. Include successful implementation of OIG recommendations as a performance metric for Senior Executive Service employees and other senior management officials.
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.
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.
19. Limit access to the underlying database and the data extraction tool to those with a bona fide need for access.
20. Create a searchable online public database with scrubbed Clearinghouse data to reduce the number of individual Clearinghouse information requests that are processed.
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.
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.
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.
24. Require additional training for Clearinghouse supervisory staff, up to and including the AED for EPHA, on effective review of Clearinghouse staff output.
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.
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.
27. Require supervisory review of all completed Clearinghouse data requests.

28. Use the data from the tracking system to develop and publish annual statistics related to the work of the Clearinghouse.
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.
30. Enforce Principle of Least Privilege and limit access to data on the P-drive to individuals with a bona fide "need to know."
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.
32. Determine, document, and implement a structure for the Clearinghouse.
33. Determine, document, and implement the role of the Freedom of Information Act Office in responding to Clearinghouse requests.
34. Require the Office of Human Resources Management (Human Resources) to provide consultation to ensure that the organizational structure in EPDSI 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.
35. Implement the recommendations from the Human Resources study.
36. Complete and document the results of a risk assessment of Clearinghouse operations.
37. Design, document, and implement control activities to respond to the results of the completed risk assessment process.
38. Develop and implement written guidance on the importance of the statements of assurance process and the related documentation requirements.
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.
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.

APPENDIX D: Management Response

MANAGEMENT RESPONSE TO REPORT OF INVESTIGATION
2019 CLEARINGHOUSE DATA BREACH
September 22, 2020

Findings:

1. Allegations of Undue Consumer Reports Influence
2. Allegations of Intentional or Malicious Disclosures
3. Allegations of Threats

Recommendations: The Inspector General found no evidence to support these allegations and thus makes no recommendations.

Management Response: Management concurs with the findings.

Findings:

4. The BRT had incomplete information at the time of its breach review in 2019.
5. The CPSC did not comply with its Breach Response Policy, specifically the CPSC has not:
    - maintained the required identity and credit monitoring as well as related services
    - tracked, documented, and disseminated a lessons learned report from this breach
    - completed an annual tabletop exercise
    - completed an annual plan review

Recommendations: The IG recommends that management:

1. Reconvene the BRT to assess the full extent of the breach, and base its response on the totality of the breach.
2. Establish blanket purchase agreements for identity monitoring, credit monitoring, and other related services for data breach victims.
3. Complete and publish a document describing lessons learned after the BRT completes its work related to this 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.
5. Conduct an annual Breach Response Policy plan review.

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.

Management Response: Management generally concurs that the BRT should convene to address the broader scope of potential breach issues identified in the OIG report, with respect to Saferproducts.gov in particular and issues of encryption more generally. Management notes that emails related to SaferProducts.gov did not fall within the scope of staff's review of the Clearinghouse data breach, and therefore staff did not consider any potential issues related to SaferProducts.gov nor whether emails were properly transmitted through appropriate encryption methods. The report indicates that the majority of emails the IG identified as problematic involved transmitting protected data outside of CPSC's domain via unencrypted email. Management notes, however, that the scope of its inquiry into the Clearinghouse data breach did not include issues related to proper encryption and focused instead on the disclosure of information similar in nature to that disclosed to Consumer Reports, meaning the majority of emails the IG identified as problematic were not within the scope of CPSC's review. In light of the issues identified in the report, Management concurs that an evaluation of additional potential issues related to SaferProducts.gov as well as whether proper encryption methods were employed is appropriate at this time. By convening the BRT, Management will evaluate the additional issues identified in the report. Management generally concurs with the recommendation that the agency should comply with its Breach Response Policy and will takes steps to review procedures and policies consistent with the recommendations above to ensure compliance.

Finding:

6. The CPSC did not present a consistent and accurate message to the public and members of Congress.

Recommendations: The IG recommends that management:

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.
8. The crisis communication plan should include annual tabletop exercises and annual plan reviews.
9. The CPSC should document the results of each crisis communication plan annual tabletop exercise.
10. The CPSC should publish the resulting comprehensive crisis communication plan after any update.

Management Response: Management generally concurs that it should develop a comprehensive crisis communication plan to ensure information is communicated accurately and consistently. Management notes that available information about the

status of the unauthorized disclosure developed over a period of time, which accounts for evolving messaging from the agency and perhaps perceived inconsistencies in specific details. In addition, the IG report addresses issues, such as emails sent in connection with Saferproducts.gov and encryption of emails, that were not within the scope of issues considered by Management as related to the Clearinghouse breach. Management provided materially accurate information consistent with its focus on the disclosure of information that was substantially similar to that disclosed to Consumer Reports, among others. Management nevertheless concurs that the development of a crisis communication plan likely will improve agency messaging and reduce potential inconsistencies in any future crisis situation, and is also convening the Breach Response Team to assess the expanded scope of issues identified by the IG, including disclosures related to SaferProducts.gov and transmission of unencrypted emails.

Finding:

7. The quality of the CPSC's response to the data breach was adversely affected by having employees who were responsible for the data breach in charge of responding to the data breach. The CPSC relied on incomplete and incompletely explained data in its reporting to the public.

Recommendations: The IG recommends that management:

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.

Management Response: Management generally concurs that convening the BRT to evaluate the expanded scope of issues identified by the OIG, including those related to encryption and SaferProducts.gov, will help contextualize and describe the extent of the data breach. The BRT does not include any of the employees who were responsible for the Clearinghouse breach. Management notes that the staff review focused on determining the extent of any Clearinghouse disclosures that were similar in nature to the disclosures that triggered the investigation. To the extent that the OIG looked through a broader lens at additional issues related to the transmission of protected data via unencrypted emails outside of CPSC's domain as well as improper internal access to protected information, Management concurs that it will evaluate those additional issues.

Finding:

8. The CPSC relied on and reported incomplete and inaccurate data and did not perform adequate due diligence and oversight of the work of Clearinghouse staff in reporting breach statistics.

Recommendations: The IG recommends that management:

12. Review all available data and establish an accurate identification of all data inadvertently released, internally and externally from 2010 to 2019.
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.
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.

Management Response: Management generally concurs that the work of Clearinghouse staff would have benefited from enhanced due diligence and oversight. Management notes, however, that the scope of potential data breaches identified in the OIG report included issues, such as potential encryption violations, that were not the subject of the review by Clearinghouse staff. Thus, staff reporting did not necessarily reflect inaccurate or materially incomplete reporting but a difference in scope and definition of the issues under review. Management has not been provided copies of the communications deemed problematic and thus does not have enough information at this time to comment on the specific concerns raised in the OIG report. Going forward, the BRT, which is comprised of staff not part of the Clearinghouse, will convene to determine, to the extent possible, the nature and extent of problems outlined by the IG and to recommend remedial measures as warranted.

Finding:

9. The CPSC has a history of concurring with but not promptly implementing audit recommendations.

Recommendations: The IG recommends that management:

15. Establish a process for communicating and enforcing the implementation of recommendations previously agreed to by management, as required by law.
16. Include successful implementation of OIG recommendations as a performance metric for Senior Executive Service employees and other senior management officials.

Management Response: Management generally concurs that specific audit recommendations have not always been implemented promptly. Management states that, whenever possible, it seeks to concur generally with an OIG recommendation because improving agency operations and functions is an iterative process, in which continual improvement is an important goal. Management believes, however, that a general concurrence with a recommendation does not commit the agency to a prescribed course of action. The ability to implement recommendations is a complex process that is affected by a multiplicity of factors, including budget constraints, staffing limitations, changed circumstances, evolving technologies, among others. As a result, Management may express a general concurrence with a recommendation to

reflect a commitment to reach a desired outcome or goal and achieve the spirit of the recommendation rather than commit to a specific prescribed approach, particularly when that goal may be achieved through a number of alternative approaches. Management seeks to continue to work cooperatively with the OIG, and has reflected the importance of working with the OIG by including the following element in all SES performance reviews: Executes appropriate actions within area of authority to address findings from the Inspector General.

Findings:

10. The CPSC maintains multiple data extraction tools because no one tool fully meets the agency's needs. The first has limited search capability but more adequately protects 6(b) information and PII data. The second is defaulted to release restricted information but has more search capabilities. The third tool is rarely used because most staff have not been trained in its use.
11. Clearinghouse staff were unable to provide evidence of the existence of implemented policies and procedures related to responding to data requests, use of data extraction tools, or requirements and methodologies to protect 6(b) information and PII data.
12. Manually reviewing the responses to data requests, which can include thousands of rows of information, leads to an unreasonably high risk of restricted information being released to the requestor.

Recommendations: The Inspector General recommends that management:

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.
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.
19. Limit access to the underlying database and the data extraction tool to those with a bona fide need for access.
20. Create a searchable online public database with scrubbed Clearinghouse data to reduce the number of individual Clearinghouse information requests that are processed.
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.
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.

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.
24. Require additional training for Clearinghouse supervisory staff, up to and including the AED for EPHA, on effective review of Clearinghouse staff output.
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.
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.
27. Require supervisory review of all completed Clearinghouse data requests.
28. Use the data from the tracking system to develop and publish annual statistics related to the work of the Clearinghouse.
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.
30. Enforce Principle of Least Privilege and limit access to data on the P-drive to individuals with a bona fide "need to know."

Management Response: Management generally concurs with these recommendations and has taken steps to implement many process improvements, including staff training on requirements to protect 6(b) information and PII data, the development and publication of an online clearinghouse dataset, https://cpsc.gov/data, and securing mid-year funding to develop a searchable online public database with scrubbed Clearinghouse data.

Finding:

13. Management neither designed nor implemented Clearinghouse internal controls adequate to meet any of the seventeen principles associated with the five components of internal control. The CPSC relied on and reported incomplete and inaccurate data and did not perform adequate due diligence and oversight of the work of Clearinghouse staff in reporting breach statistics.

Recommendations: The IG recommends that management:

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.
32. Determine, document, and implement a structure for the Clearinghouse.

33. Determine, document, and implement the role of the Freedom of Information Act Office in responding to Clearinghouse requests.
34. Require the Office of Human Resources Management (Human Resources) to provide consultation to ensure that the organizational structure in EPDSI 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.
35. Implement the recommendations from the Human Resources study.
36. Complete and document the results of a risk assessment of Clearinghouse operations.
37. Design, document, and implement control activities to respond to the results of the completed risk assessment process.
38. Develop and implement written guidance on the importance of the statements of assurance process and the related documentation requirements.
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 MIS Code.
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.

Management Response: Management generally concurs that the work of Clearinghouse staff would have benefited from enhanced due diligence and oversight, and that Clearinghouse internal controls were not adequate. Management notes, however, that the scope of potential data breaches identified in the OIG report included issues, such as potential encryption violations, that were not the subject of the review by Clearinghouse staff. Thus, staff reporting did not necessarily reflect inaccurate or materially incomplete reporting but a difference in scope and definition of the issues under review. Management generally concurs with these Recommendations and has taken steps to implement many of these process improvements, including developing written guidance on the statements of assurance process and holding training on its importance, as well as working with the Office of General Counsel to develop guidelines for the appropriate release of information.

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
Consumer Product Safety Commission
4330 East-West Highway, Room 702
Bethesda MD 20814