UNITED STATES
CONSUMER PRODUCT SAFETY COMMISSION

OFFICE OF INSPECTOR GENERAL

CONSUMER PRODUCT SAFETY IMPROVEMENT ACT OF 2008, SECTION 212 STATUTORY COMPLIANCE AUDIT

ISSUED SEPTEMBER 21, 2012

UNITED STATES
CONSUMER PRODUCT SAFETY COMMISSION
BETHESDA, MD 20814

Memorandum

Date: September 21, 2012

TO : Inez Moore Tenenbaum, Chairman
Nancy A. Nord, Commissioner
Robert S. Adler, Commissioner
Anne Meagher Northup, Commissioner

FROM : Christopher W. Dentel
Inspector General

SUBJECT : Compliance Audit of the Implementation and Establishment of the CPSC's Publically Available Consumer Product Safety Information Database

The Office of Inspector General has completed its audit of the CPSC's Publically Available Consumer Product Safety Information Database. A copy of the report is attached.

Management (EXIT) has been briefed regarding the findings and recommendations of this audit and given an opportunity to respond to them. Management concurred with the findings and has already implemented all necessary corrective actions. Management's responses concurring with the audit's findings are summarized throughout the report.

If you have any questions about this report or wish to discuss it, please feel free to contact me at 301-504-7644 or cdentel@cpsc.gov.

Christopher W. Dentel
Inspector General

TABLE OF CONTENTS

EXECUTIVE SUMMARY

BACKGROUND

The U.S. Consumer Product Safety Commission's (CPSC) Office of Inspector General (OIG) conducted a compliance audit of the implementation and establishment of the CPSC's publically available consumer product safety information database. The database is mandated by the Consumer Product Safety Improvement Act of 2008 (CPSIA), which was enacted on August 14, 2008.

The CPSIA requires the CPSC to implement a publicly accessible, searchable database of consumer product incident reports. The purpose of the database is to provide a single central location where consumers can report incidents (known as Reports of Harm) and search for prior incidents/recalls. Additionally, the database provides the manufacturers, private labelers, and importers of the products in question with the ability to comment on the Reports of Harm submitted. For example, the manufacturer can use the comment functionality within the database to comment on actions taken to remediate product safety concerns or to rebut a Report of Harm. Moreover, if they believe that the information provided in a Report of Harm contains confidential information or is materially inaccurate, businesses can use the database to request that the CPSC correct Reports of Harm submitted by consumers.

The database is an integral part of the overall CPSC IT Modernization effort, known as the Consumer Product Safety Risk Management System (CPSRMS). The implementation of the CPSRMS will occur over the next 2 to 3 years, and as of January 18, 2011, it was estimated to cost approximately $67.6 million.[1]

Pursuant to section 6A(a)(3) of the CPSIA, the CPSC was required to submit the implementation plan for the database to Congress within 180 days of the enactment of the CPSIA. However, the plan was not submitted until September 10, 2009, some 392 days after the CPISA's enactment.[2] The CPSIA also required that the database be established within the 18-month period following the CPSC's submission of the implementation plan to Congress. The public database was launched to the public on March 11, 2011.

RESULTS OF EVALUATION AND FINDINGS

This report covers the CPSC's implementation of the publically available consumer product safety information database, and it assesses the database's compliance with Section 212 of the CPSIA. Overall, we found that the CPSC has substantially complied with the requirements of the CPSIA for the database. However, we did note one instance in which personal information regarding a consumer (name, contact, and medical information), had been made available to the

---

[1] According to the Capital Asset Plan and Business Case Summary, provided to the OMB on January 18, 2011, the total estimated CPSRMS life cycle cost, including Steady State and Full-Time Equivalents costs, is $67,643,000. This amount includes actual amounts of $8,955,000 for 2009 and $11,476,000 for 2010; and estimated amounts of $11,980,000 for 2011; $10,316,000 for 2012; $7,440,000 for 2013; $5,784,000 for 2015; and $5,845,000 for 2015 and beyond. The estimated cost agreed to the President's Budget, submitted on January 18, 2011. According to the President's Budget, the total Agency funding for CPSRMS in FY 2010 was $10,135,000 for the Development, Modernization, and Enhancement costs and $1,341,000 for the Steady State costs.

[2] CPSC management chose not to submit the database implementation plan to Congress until secure funding was available. The CPSC did this to ensure it would have sufficient resources to implement the Database.

public. The type of information in question is characterized by the government as Personally Identifiable Information (PII), and its actual or potential unauthorized release is referred to as a breach of PII.

This particular breach of PII occurred because the CPSC did not properly conceal or redact the PII contained in a publically available Report of Harm. The breach in question was not discovered until a public user of the database notified the CPSC that a Report of Harm on the database contained an attachment that included the report submitter's name and phone number. The attachment also included a Web link to the report submitter's website, which included additional PII. The individual responsible for "scrubbing" the files to remove PII data before they were posted did not follow proper procedures. Instead, the individual attempted to redact the PII contained in the report by using Microsoft Word (the program that had also been used to generate the attachment) to add objects (black rectangles) to cover the PII information in the attachment. However, the objects were alterable by public users of the database, rendering the redaction meaningless and the information underneath viewable.

RECOMMENDATION

Upon notification of the PII breach, the CPSC acted to prevent similar situations from occurring in the future by restricting the database's public users from posting Microsoft Word (.doc and .docx file extensions) attachments to Reports of Harm. As such, all attachment submissions are now formatted in Adobe (.Pdf file extension). This eliminated the ability of those charged with "scrubbing" PII from the files to add "objects" to attachments in an attempt to redact information submitted and it effectively forces them to follow proper procedures and make permanent redactions.

AUDITEE COMMENTS

The auditees concurred with our finding and immediately remediated the issue, as well as, instituted new procedures to prevent additional occurrences.

INTRODUCTION

BACKGROUND

The Consumer Product Safety Commission Public Database

Section 212 of the CPSIA, requires the CPSC to implement a publicly accessible, searchable database of consumer product incident reports. Pursuant to section 6A(a)(3) of the CPSIA, the establishment of the database must occur within the 18-month period following the CPSC's submission of a plan to Congress regarding the Database implementation as required under section 6A(a)(2). The CPSC submitted this plan to Congress on September 10, 2009 and the database was launched March 11, 2011. The database is an integral part of the overall CPSC IT Modernization effort, known as the Consumer Product Safety Risk Management System (CPSRMS). The CPSRMS implementation will occur over the next two to three years.

The database includes three key modules: Consumer/Public Portal, Industry Partner (Business) Portal, and Incident Management Control Center (IMCC). The Consumer Portal allows public users to submit Reports of Harm to the CPSC for review. The Business Portal allows manufactures, private labelers, and importers to submit comments on Reports of Harm made by the Public. The IMCC allows CPSC internal users to review and process the Reports of Harm along with their related comments. The IMCC module also aides the CPSC in performing other administrative tasks within the database.

The CPSIA, Section 212 Requirements

Section 212 of the CPSIA, sets-out the following requirements regarding the implementation and operation of the database:

Content – As required by the CPISA, consumers, local, State, or Federal government agencies, health care professionals, child service providers, and public safety entities can submit Reports of Harm relating to the use of consumer products and other products or substances regulated by the CPSC to the CPSC. The database is required to contain all Reports of Harm submitted to the CPSC on or after March 11, 2011. Each publically viewable Report of Harm must contain the specific categories of information outlined in the CPSIA, such as the description of the product, the manufacture's name, etc. The database must also contain information derived from businesses that has been previously released to the public by the CPSC relating to the voluntary corrective actions businesses have taken in consultation with the CPSC. Finally, the database must contain a clear and conspicuous notice that the CPSC does not guarantee the accuracy, completeness, or adequacy of the contents of the Database.

Organization – The CPSC is required to categorize the information maintained in the database in "a manner consistent with the public interest." The database must include functionality that allows the sorting of the database information by publication date of the Report of Harm, the product name, the model name, and the manufacture/private labeler name.

Procedural – The CPSC is required to implement the following processes: 1) A process must be in place to ensure transmittal of Reports of Harm to businesses within five business days of the CPSC's review, where practicable, and the Reports of Harm must be posted for public viewing within 10 business days of being transmitted to the business. 2) The CPSC must also implement

a process to allow businesses the opportunity to comment on the Reports of Harm and for the publication of those comments to the database to occur at the same time as the Report of Harm, where practicable. 3) A process must be in place to enable businesses to notify the CPSC in the event confidential or materially inaccurate information is contained within the Reports of Harm. In those situations where confidential or materially inaccurate information is present in a Report of harm, the CPSC must implement a process to redact, remove, or correct said reports. 4) Finally, the CPSC is required to limit access to any Personally Identifiable Information (PII) provided by the report submitter. Only the businesses expressly authorized by the submitters are allowed to access the submitter's contact information. In these cases, the information contained in the Reports of Harm is for verification purposes only.

OBJECTIVE

The primary objective of this audit is to determine whether the CPSC has implemented the publically available database of consumer product safety information in accordance with the requirements stipulated by Section 212 of the CPSIA.

SCOPE

This audit covers the public database implementation and its establishment as of March 11, 2011 by various offices of the CPSC located in Bethesda, Maryland. The performance of fieldwork for this audit was conducted from April 2011 through June 2011.

METHODOLOGY

This audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To accomplish our audit objectives, we first gained an understanding of the CPSIA's requirements regarding the database implementation. This understanding was attained through obtaining and reviewing the CPSIA legislation and key reports developed by the CPSC management (and their independent contractors), which documented the databases implementation. Based on this understanding, we were able to identify the following implementation requirements, set forth by Section 212 of the CPSIA:

- CPSRMS required Content
- Notice Requirements
- Availability of Contact Information
- Information Submission Process
- Organization of Database
- Transmission of Reports to Manufactures and Private Labelers
- Manufacture/Private Labeler's Opportunity to Comment
- Publication of Reports and Comments
- Upgrade of Commission Information Technology Systems

For each area noted above, we conducted interviews and walkthroughs with key personnel from the Office of Information and Technology (EXIT) and the Office of Hazard Reduction and Identification (EXHR). This was done to help us gain an understanding of the impact of the above requirements on the processing of a Report of Harm and to determine the CPSC's compliance with the related CPSIA, Section 212 content and organizational requirements. Additionally, we obtained a population of Reports of Harm published to the database as of March 11, 2011 through April 19, 2011 from the Database Administrator (DBA). We performed analytical procedures over this population to determine whether the CPSC complied with the various procedural requirements of CPSIA, Section 212.

RESULTS AND FININGS

Overall, we found that the CPSC has substantially complied with all the statutory requirements of the CPSIA for the publically available database. However, we did note one instance of a breach of PII in a published Report of Harm.

PII Breach on May 3, 2011

The CPSIA at Section 212, paragraph 6A(6), *Availability of Contact Information*, states, "The Commission may not disclose, under this section, the name, address, or other contact information of any individual or entity that submits to the Commission a report described in paragraph (1)(A), except that the Commission may provide such information to the manufacturer or private labeler of the product with the express written consent of the person submitting the information. Consumer information provided to a manufacturer or private labeler under this section may not be used or disseminated to any other party for any purpose other than verifying a report submitted under paragraph (1)(A)." As detailed below, the CPSC failed to comply with this requirement when it failed to properly redact information provided by an individual that submitted a Report of Harm.

The breach involved an attachment in a Report of Harm that contained the report submitter's name and phone number. The attachment also included a link and the username and password to a website that the report submitter developed that contained medical information about the submitter. The type of information in question is characterized by the government as Personally Identifiable Information (PII) and its actual or potential release constitutes a breach of PII.

The breach in question was not discovered until a public user of the database notified the CPSC that a Report of Harm on the database contained a Microsoft Word attachment which contained the report submitter's name, phone number and an attachment which contained a web link to the to the report submitter's website which included additional PII.

The CPSC employee responsible for "scrubbing" Reports of Harm to remove PII data before they were posted did not follow proper procedures. Instead, the individual attempted to redact the PII contained in the report by adding objects (black rectangles) to cover the information in the Microsoft Word file. However, the objects were alterable by public users of the database, rendering the information underneath viewable. As result of the breach of PII, the report submitters personal contact and medical information were made publically available in the database

The member of the public who discovered the breach of PII notified the CPSC's Information Center of the issue on Thursday May 5, 2011 at 2:59 AM. The Information Center followed up with the breach reporter several times that day to clarify the incident and to obtain additional information. The next morning, Friday May 6, 2011 at 10:14 AM, the Information Center notified the Consumer Information Systems Support team, who a few minutes later contacted the appropriate business resources to remediate the issue. However, due to a misunderstanding with the business contact, the remediation of the issue did not occur until the following Monday evening at 8:22pm, May 9, 2011 when the business contact contacted the CPSC Information System Security Officer (ISSO). The ISSO then notified the CPSC Inspector General of the breach, as the agency was required to do.

RECOMMENDATION

Upon notification of the PII breach, the CPSC acted to prevent similar situations from occurring in the future by developing new standard operating procedures regarding redacting PII from Reports of harm and restricting the database's public users from posting Microsoft Word (.doc and .docx file extensions) attachments to Reports of Harm. As such, all attachment submissions are now formatted in Adobe (.Pdf file extension) only. This eliminates the ability of those charged with "scrubbing" PII from the files to add, "objects" to attachments when redacting information from Reports of Harm and forces them to follow proper procedures.