UNITED STATES CONSUMER PRODUCT SAFETY COMMISSION

OFFICE OF INSPECTOR GENERAL

CYBERSECURITY INFORMATION SHARING ACT OF 2015 REVIEW REPORT

ISSUED: 8/14/2016

The report is in response to the Cybersecurity Information Sharing Act of 2015 (P.L 114-113), which requires the CPSC OIG to complete an assessment of the CPSC's policies, procedures and practices that protect systems containing personally identifiable information.

U.S. CONSUMER PRODUCT SAFETY COMMISSION
BETHESDA, MD 20814

Christopher W. Dentel
Inspector General

Tel: 301 504-7644
Fax: 301 504-7004
Email: cdentel@cpsc.gov

Date: August 14, 2016

TO : Elliot F. Kaye, Chairman
Robert S. Adler, Commissioner
Marietta S. Robinson, Commissioner
Ann Marie Buerkle, Commissioner
Joseph P. Mohorovic, Commissioner

FROM : Christopher W. Dentel
Inspector General

SUBJECT : Cybersecurity Information Sharing Act of 2015 Review

The Cybersecurity Information Sharing Act of 2015, Title IV, Section 406 (hereinafter referred to as "the Cybersecurity Act") requires that the U.S. Consumer Product Safety Commission's (CPSC) Office of Inspector General (OIG) conduct an independent evaluation of the CPSC's establishment of information security policies, procedures, and practices that protect agency systems that provide access to personally identifiable information (PII).

The primary purpose of our evaluation was to determine if the CPSC had established the policies, procedures, and practices required by the Cybersecurity Act for agency systems that contain PII and to transmit a description of same to Congress. Additionally, we were charged with evaluating whether appropriate standards regarding logical access policies and practices were followed. We were not charged with making an assessment regarding the overall effectiveness of the policies, procedures, and practices in question.

This evaluation was not an audit; therefore, it was not performed in accordance with generally accepted government auditing standards. The OIG conducted this review in accordance with the Council of Inspectors General on Integrity and Efficiency (CIGIE), Quality Standards for Inspection and Evaluation. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our objectives.

Overall, we found that the CPSC has established policies, procedures, and practices for logical access, contractor oversight, forensics, and software inventory. However, as detailed in the report, based on the information provided by management, we noted management had not achieved a number of the requirements set forth in the Cybersecurity Act, including: the development of logical access policies and procedures for all agency systems that permit access to PII; the universal enforcement of smartcard authentication across all functions; the implementation of a standard software inventory methodology; and the development of formal procedures and automated practices for software license management.

Agency management generally concurred with our findings and recommendations. The management response to our report has been included as an appendix to our report.

A number of the issues raised in this report will be addressed in greater in detail in the Federal Information Security Management Act review currently underway. Should you have any questions, please feel free to contact me.

Christopher W. Dentel
Inspector General

Table of Contents

Appendices E – I are confidential

EXECUTIVE SUMMARY

OBJECTIVE

Our sole objective was to report on the Consumer Product Safety Commission's (CPSC) establishment of information security policies, procedures, and practices that protect agency systems that provide access to personally identifiable information (PII), as set forth in the *Cybersecurity Information Sharing Act of 2015*, Title IV, Section 406 (hereinafter referred to as "the Cybersecurity Act").

BACKGROUND

On December 15, 2015, the President signed into law the Cybersecurity Act *(Public Law 114-113)*, as part of the Consolidated Appropriations Act of 2016. This Act requires Federal Agencies to establish policies, procedures, and practices to protect Federal computer systems that house PII.

Under Section 406 of the Cybersecurity Act, our office is required to:

- Report the CPSC's management assertions about the establishment of the CPSC's policies, procedures and practices related to logical access, multifactor authentication for privileged users, software inventory/license compliance, data exfiltration, and the identification of "other threats"

- Evaluate if management followed the appropriate standards for logical access policies, procedures, and practices.

We are also required to report the results of this evaluation to congress no later than 240 days after the enactment of this legislation. This report satisfies that requirement.

RESULTS OF EVALUATION AND FINDINGS

This report addresses the requirements placed upon the CPSC OIG by the Cybersecurity Act. Overall, we found that the CPSC has established policies, procedures, and practices for logical access, contractor oversight, forensics, and software inventory. However, based on the information provided by management[1], we noted management has not achieved the following requirements set forth in the Cybersecurity Act:

- Development of logical access policies and procedures for all agency systems that permit access to PII;
- Universal enforcement of smartcard authentication across all functions;
- Implementation of a standard software inventory methodology; and
- Development of formal procedures and automated practices for software license management.

Management has reported that it has established forensics and visibility procedures and practices to assist with identifying and monitoring data exfiltration. Management does not have capabilities in place to manage data rights or ensure data loss prevention[2]. Existing CPSC logical access policies, procedures, and practices address many required elements but do not comply with all of the appropriate standards, as follows:

- Existing access control policies and Standard Operating Procedures (SOPs) do not consistently:
  - establish a process for revoking access rights,
  - include procedures for the modification of account privileges, and
  - include procedures that define what Account Managers must do to monitor the use of information system accounts or assign Account Managers to perform these tasks.

- The Consumer Product Safety Risk Management System (CPSRMS) access control SOP is based on an out of date version of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev. 3 versus Rev. 4.

- Existing CPSC access control procedures do not adequately address the use and control of shared network accounts. Specifically, management has not established a process for reissuing shared account credentials when individuals separate from the agency or when they no longer have a business need for this access.

- The General Access Control policy states, "*The GSS LAN and all Major Applications must have defined conditions for group/role membership.*" The current policy requires access to be granted by system owner but the specific criteria are not formally documented in all system SOPs.

[1] See Appendices E-I for the information provided by management.

[2] Note: The Federal Information Security Modernization Act of 2014 does not compel agencies to implement data rights management and data loss prevention capabilities.

RESULTS AND FINDINGS

LOGICAL ACCESS POLICIES, PROCEDURES, AND PRACTICES

According to the Government Accountability Office's, Federal Information Systems Control Manual, "*Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them from unauthorized modification, loss, and disclosure...Logical access controls require users to authenticate themselves (through the use of secret passwords or other identifiers) and limit the files and other resources that authenticated users can access and the actions that they can execute.*" Management has not dedicated the resources required to the task of establishing and implementing logical access policies and procedures. Currently, the CPSC does not centrally control all logical access. Therefore, it is difficult for management to ensure the consistent establishment and application of these policies and procedures. This may result in users gaining inappropriate and anonymous access to agency information systems containing PII. The CPSC can improve its ability to protect PII by documenting new and enhancing existing logical access policies, procedures, and practices.

Based on our review of applicable systems, we identified the following areas of improvement:

- Development of logical access policies, procedures, and practices for all of the agency systems that permit access to PII:

    - Management has developed policies, procedures, and practices for the CPSC's General Support System Local Area Network (GSS LAN) and systems that management has defined as major applications. While management intended these policies and procedures to cover all CPSC systems the scope of these General Access Controls do not cover all of the CPSC systems that permit access to PII, in particular, they do not cover those systems provided by third party service providers, and management has not developed procedures for all agency systems that contain PII. In addition, the existing logical access policies and procedures do not address all of the requirements found in the most current revision of NIST SP 800-53.

- Existing logical access policies, procedures, and practices do not comply with all of the appropriate standards. We identified the following information missing from existing information systems' policies and procedures:

    - GSS LAN policies and procedures do not specifically define aspects of:
        - how quickly user accounts must be revoked upon notification of a change in user responsibilities;
        - procedures for revoking contractor accounts;
        - conditions for the group/role membership;
        - how account managers will monitor the use of network accounts; and
        - the use and control of shared network accounts – Specifically, management has not established a process for reissuing shared account credentials when individuals separate from the agency or when they no longer have a business need access.

    - The CPSRMS access control policies and procedures have not been updated to reflect

the most recent version of NIST SP 800-53 (Rev 4) Additionally, these policies/procedures do not include the following criteria which were required in Rev 3 as well as Rev 4:

- how quickly accounts must be revoked upon notification of the user's separation/change in responsibilities; and
- procedures for modifying user account privileges.

- Dynamic Content Management (DCM) policies and procedures do not define:
  - procedures for modifying user account privileges;
  - conditions (business justifications) for the group/role membership or access authorizations (i.e., privileges) and other attributes, as required, for each account;
  - procedures for monitoring the use of DCM accounts and the assignment of account managers to monitor the use of DCM accounts; and
  - the use and control of shared DCM accounts – Specifically, management has not established a process for reissuing shared account credentials when individuals separate from the agency or when they no longer have a business need for this access.

- International Data System Risk Assessment Methodology (ITDSRAM) policies and procedures do not define:
  - how quickly accounts must be revoked upon notification of the user's separation/change in responsibilities;
  - procedures for modifying user account privileges; and
  - procedures for monitoring the use of ITDSRAM accounts and the assignment of account managers to monitor the use of ITDSRAM accounts.

Recommendation:
We recommend CPSC's management develop, document, and formalize processes and practices to ensure the implementation of all requisite logical access controls. This includes:

1. The development of logical access control policies and procedures for all systems that permit access to PII that are not currently covered by existing policies and procedures. The CPSC can achieve this by establishing an entity-wide logical access policy for all agency systems or by developing tailored logical access policies for those systems containing PII.

2. Provide training or support to individual system owners, where necessary, on how to establish, implement, and maintain logical access policies and procedures for systems that contain PII.

3. The following elements should be included in the General Access Control Policy and attendant procedures:
   - ✓ An updated process for revoking access that includes the following additions:
     - how quickly all user accounts must be revoked upon notification of a change in user responsibilities;
     - the process for revoking contractor network user accounts

- how quickly ITDSRAM and CPSRMS user accounts must be revoked upon notification of the user's separation;

- ✓ The ITDSRAM, CPSRMS, and DCM SOPs should include procedures for the modification of account privileges.
- ✓ Formalize and document the conditions for group/role membership for the GSS LAN and DCM.
- ✓ Update the CPSRMS access control SOP to reflect NIST SP 800-53, Rev. 4 requirements.
- ✓ The existing SOPs should consistently assign account managers to monitor the use of information system accounts and consistently define how management monitors the use of information system accounts. Specifically:
  - The CPSC Audit and Accountability policy should assign account managers to monitor the use of network accounts;
  - The DCM access control SOP should reference information system account monitoring and management should develop an Audit and Accountability SOP for DCM.
  - The ITDSRAM access control SOP should describe the activities account managers must perform to monitor the use of information system accounts and management should assign account managers to monitor the use of information system accounts.
- ✓ The CPSC access control procedures should adequately address the use and control of shared network and DCM accounts. Specifically, management should establish a process for reissuing shared account credentials when individuals separate from the agency or when they no longer have a business need for this access.

SOFTWARE INVENTORY AND LICENSE MANAGEMENT POLICIES, PROCEDURES AND PRACTICES

Active management of an organization's software inventory is critical to ensuring the confidentiality, integrity, and availability of agency data and systems. Further, proper software inventory processes ensure the installation of authorized software that can execute on an organization's network and the timely identification and removal of malicious/unauthorized software. CPSC has policies and procedures for managing the acquisition and installation of software. CPSC also has tools and the ability to identify installed software and versions on equipment to address malicious or unauthorized software. According to the information provided by management, the CPSC has not established policies, procedures, and practices for software inventory and license management. Specifically, management stated, "*The agency does not currently have an automated practice for tracking software licenses that are installed on covered information systems.*" Instead, license management activities are ad hoc and are performed on an as needed basis. In addition, management has not adopted a standard software inventory methodology that supports agency operations and license management requirements. Although not documented in management's original response, management asserts that a comprehensive inventory could be created using tools currently in use. However, this has never been done and doing so would require significant manual consolidation. Management has opted

to postpone development of this capability pending determination of "*…eventual software procurements associated with the DHS Continuous Diagnostic & Monitoring (CDM) program.*"

Inadequate software inventory management results in noncompliance with the Federal Information Security Management Act (FISMA) and prevents management from ensuring adequate control for CPSC owned PII.

Recommendation:

1. We recommend management develop, document, and formalize software inventory and license management policies and procedures.

MANAGEMENT DOES NOT SYSTEMATICALLY ENFORCE SMARTCARD AUTHENTICATION

According to the Department of Homeland Security's Homeland Security Presidential Directive 12 (HSPD-12) website[3], "*There are wide variations in the quality and security of identification used to gain access to secure facilities where there is potential for terrorist attacks. In order to eliminate these variations, U.S. policy is to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). This directive mandates a federal standard for secure and reliable forms of identification.*"

In support of this mandate, NIST released Federal Information Processing Standards 201-2 (FIPS 201-1) which compels the use of smartcard authentication across the U.S. government. In an effort to comply with these requirements, last year management began to enforce smartcard authentication systematically. After initial implementation, management identified conflicts with system patching that would result in increased risk for the agency and decided to remove the technical controls enforcing smartcard authentication. Currently, management provides smartcard authentication for logical access to endpoints across the agency and the majority of these users rely solely on the use of the smartcard to authenticate to the network. However, as management does not enforce smartcard authentication systematically; malicious actors who are able to compromise these single-factor credentials may be able to gain unauthorized access to the network, and management does not comply with HSPD-12.

Recommendation:

1. We recommend management comply with HSPD-12 and implement technical controls outlined in FIPS 201-2 to enforce multifactor authentication supported by the Personal Identity Verification Card.

[3] https://www.dhs.gov/homeland-security-presidential-directive-12

APPENDIX A: BACKGOUND

BACKGROUND

The CPSC OIG conducted the evaluation of the CPSC's policies, procedures, and practices described in Title IV, Section 406, of the Cybersecurity Act. The Cybersecurity Act requires Federal agencies to establish information security policies, procedures, and practices that protect agency systems that provide access to PII. Specifically, the Act requires Inspectors General to report on the establishment of the policies, procedures, and practices related to logical access, multifactor authentication for privileged users, software inventory and license compliance, data exfiltration and the identification of "other threats." The OIG is required to include the information collected from CPSC management for each of these topics in this report and to evaluate if management has followed the appropriate standards for the logical access policies, procedures, and practices. The Office of Information Technology (EXIT) provides governance over the CPSC's information security program and administers logical access for many CPSC systems. Program officials within the CPSC departments administer logical access for agency systems when EXIT does not provide administrative support.

The information systems covered by this evaluation are described below:

- ✓ *GSS LAN*

The GSS LAN is the CPSC support system that delivers client/server networking architecture, office automation, data warehousing, file storage and backup applications to support all divisions of CPSC. In addition, iManager is the primary solution used to create/revoke network user accounts. EXIT administers logical access for the GSS LAN.

- ✓ *CPSRMS*

CPSRMS is the agency's implementation of the public database mandated in the Consumer Product Safety Improvement Act 2008, Section 212. CPSRMS is comprised of three main subsystems: public portal, business portal, and incident processing. The Office of Hazard Identification and Reduction (EXHR) administers logical access for CPSRMS through integrated field teams and has restricted existing network users to use of single sign-on.

- ✓ *DCM*

The DCM system provides a common workflow across several CPSC program areas including the Office of Compliance, the Office of Field Operations, and the Office of Import Surveillance (EXIS). As with CPSRMS, EXHR administers logical access by integrated field teams and has restricted existing network users to use of single sign-on.

- ✓ *ITDSRAM*

ITDSRAM is a solution designed to automate workflow for EXIS personnel. Thus, EXIS personnel administer logical access. ITDSRAM is comprised of three main components: Data Manager, Risk Assessment Methodology applications and rules, and the ITDSRAM database.

APPENDIX B: OBJECTIVE, SCOPE & METHODOLOGY

OBJECTIVE

The purpose of our evaluation was to determine if the CPSC has established the policies, procedures, and practices required by the Cybersecurity Act for agency systems' that contain PII. Through this evaluation process, we also determined whether standards for logical access were appropriate.

SCOPE

This evaluation covered the CPSC's information security policies, procedures, and practices established as of April 15, 2016. Specifically, we reviewed the policies, procedures, and practices related to logical access controls[4], multifactor authentication for privileged users[5], software inventory and license management, data exfiltration, and other threats[6] provided by CPSC management. We did conduct any evaluation procedures to verify, analyze, or validate the data provided.

Scope limitation: Management stated that it does not maintain an inventory of agency systems containing PII or a comprehensive software inventory. Although management created a partial inventory of 19 CPSC systems that permit access to PII for this review, management was unable to assert its completeness, and the OIG noted that this inventory was incomplete.

METHODOLOGY

This evaluation was not an audit; therefore, it was **not** performed in accordance with generally accepted government auditing standards. The OIG conducted this review in accordance with the Council of Inspectors General on Integrity and Efficiency (CIGIE), *Quality Standards for Inspection and Evaluation*. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our objectives.

To accomplish our evaluation objectives, we obtained management's description of the policies, procedures, and practices established to protect agency systems that permit access to PII. Specifically, we obtained CPSC's management descriptions of:

- the logical access and software inventory/license compliance policies, procedures and practices[7];
- the controls over logical access and multifactor authentication for privileged users and management's reasons, where applicable, for not utilizing multifactor authentication for privileged users[8];

[4] According to the Act, logical access is defined as "a process of granting or denying specific requests to obtain and use information and related information processing services."
5 According to the Act, multifactor authentication is defined as "the use of not fewer than 2 authentication factors".
6 According to the Act, these "other threats" include (I) data loss prevention capabilities; (II) forensics and visibility capabilities; and (III) digital rights management capabilities.
7 See Appendices F & G.
8 See Appendices F, G & I.

- the capabilities the CPSC utilizes to monitor and detect data exfiltration and other threats, a description of how the agency uses these capabilities, and, where applicable, a description of why the agency is not using these capabilities[9];
- the policies and procedures established by the agency to ensure entities, including contractors, providing services to the CPSC are implementing the software inventory/software license compliance policies and procedures, as well as, monitoring for data exfiltration and other threats[10].

In addition, we conducted interviews with key CPSC personnel and evaluated the logical access policies, procedures, and practices to ensure that these complied with appropriate standards.

[9] See Appendices G & H.
[10] See Appendix H.

APPENDIX C: ACRONYMS & ABBREVIATIONS

CDM	Continuous Diagnostic & Monitoring program
CIGIE	Council of Inspectors General on Integrity and Efficiency
CPSC	Consumer Product and Safety Commission
CPSIA	Consumer Product Safety Improvement Act
CPSRMS	Consumer Product Safety Risk Management System
DCM	Dynamic Content Management System
DHS	Department of Homeland Security
EXHR	Office of Hazard Identification and Reduction
EXIS	Office of Import Surveillance
EXIT	Office of Information Technology
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GSSLAN	General Support System Local Area Network
HSPD 12	Homeland Security Presidential Directive 12
ITDSRAM	International Data System Risk Management Methodology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personal Identifiable Information
SOP	Standard Operating Procedure
SP	Special Publication

APPENDIX D: MANAGEMENT'S RESPONSE

PAGE INTENTIONALLY LEFT BLANK

UNITED STATES
CONSUMER PRODUCT SAFETY COMMISSION
4330 EAST WEST HIGHWAY
BETHESDA, MD 20814

Memorandum

Date: August 4, 2016

TO : Christopher Dentel
Inspector General
Office of the Inspector General

THROUGH: Patrick Manley
Chief Information Security Officer
Office of Information Technology

FROM : James Rolfes
Chief Information Officer
Office of Information Technology

SUBJECT : Management Response to Cybersecurity Information Sharing Act of 2015 Evaluation

Thank you for the opportunity to respond to the Cybersecurity Information Sharing Act of 2015 evaluation. The Office of Information Technology (EXIT) has carefully reviewed the evaluation and concurs with the findings. EXIT intends to continue efforts to further improve the agency's security posture overall and specifically for policies and procedures related to the protection of agency systems that provide access to personally identifiable information (PII).

We will review your recommendations to align them with planned actions and future work.