Office of Inspector General

U.S. Consumer Product Safety Commission

Report on the Penetration and Vulnerability Assessment of CPSC's Information Technology Systems

June 11, 2019

19-A-08

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 OIG.

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; and

Work together to address government-wide issues.

Office of Inspector General
U. S. CONSUMER PRODUCT SAFETY COMMISSION

June 11, 2019

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

FROM: Christopher W. Dentel, Inspector General

SUBJECT: Summary of Defense Point Security's Penetration Testing

To assess the security of the United States Consumer Product Safety Commission's (CPSC) information technology (IT) infrastructure, the CPSC Office of Inspector General (OIG) retained the services of Defense Point Security (DPS). Under a contract monitored by the OIG, DPS conducted a penetration and vulnerability assessment of the CPSC's IT systems. The contract required that the assessment be performed in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) *Quality Standards for Inspection and Evaluation* (QSIE).

In connection with the contract, we reviewed DPS's report and related documentation and inquired of its representatives. Our review was not intended to enable us to express, and we do not express, an opinion on the matters contained in the report. DPS is responsible for the attached report. However, our review disclosed no instances where DPS did not comply, in all material respects, with CIGIE's QSIE.

DPS obtained an understanding of CPSC systems, controls, and vulnerabilities sufficient to prioritize the risks and vulnerabilities identified. This prioritization will assist CPSC management in prioritizing the remedial actions necessary to ameliorate the IT security risks found by DPS.

DPS noted 17 findings and made 40 recommendations. Due to the sensitive nature of the information contained in their report and our desire to not provide a roadmap for penetrating the CPSC's IT security, this office is publishing a brief summary of the report rather than the report itself.

Should you have any questions, please contact me.

Report on the Penetration and Vulnerability Assessment of CPSC's Information Technology Systems

June 11, 2019

Summary

Objective

The objective of this penetration test was to assess the security of the United States Consumer Product Safety Commission's (CPSC) information technology (IT) infrastructure by identifying, cataloging, and safely exploiting security vulnerabilities. This test should assist the CPSC in identifying and prioritizing remedial efforts that will improve the agency's security posture by eliminating security weaknesses that could have a significant negative impact on the confidentiality, integrity, and availability of agency information systems and data.

Background

This engagement required the contractor, Defense Point Security (DPS), to obtain an understanding of CPSC systems, controls, and vulnerabilities sufficient to prioritize the risks and vulnerabilities identified. This prioritization will allow CPSC management to make an informed determination on which remedial steps to perform and the order in which to perform them.

The report addresses:

CPSC Cross-Cutting Strategic Priority #3:

Information Technology

Office of Inspector General Management Challenge #4:

Information Technology Security

Assessment

On the basis of our assessment, we determined that the CPSC's security controls require improvement to more effectively detect and prevent certain cyberattacks.

During the time DPS was performing its assessment, the CPSC experienced an unrelated network outage which led to a suspension of fieldwork. Also, early on in the testing phase DPS discovered improperly posted sensitive information which was publicly accessible via widely-used search engines and CPSC.gov. DPS notified the CPSC immediately about this discovery.

We shared the results of this assessment with CPSC senior management and IT staff during the engagement and at a meeting on May 6, 2019. Management generally concurred with our observations. We have addressed their comments about the report as appropriate.

We noted that the CPSC's web application protections were generally sound at the time of testing. However, as part of our wireless, internal, and physical assessments, we found multiple security risks which in combination create a substantial risk to agency systems and data.

We provided 40 actionable recommendations. These recommendations address issues of physical security, controls over sensitive information, system configuration, authentication, and other system security issues. When completed, these recommendations will significantly improve the information technology security posture of the CPSC. Management has already implemented some of the recommendations.

Appendix B: Agency Response

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

Memorandum

Date: June 6, 2019

TO : Christopher Dentel
Inspector General
Office of the Inspector General

FROM : Mary Boyle
Executive Director
Office of the Executive Director

MARY BOYLE

SUBJECT : Management Response to Report on the Penetration and Vulnerability Assessment of CPSC's Information Technology Systems

Thank you for the opportunity to review and provide a management response for the network penetration test performed March 4, 2019 through April 19, 2019. I concur with the findings and recommendations made in the report provided on May 30, 2019.

I appreciate being informed of gaps in CPSC's security system identified through this activity. Staff immediately began to take steps to address the recommendations in the report and is working diligently to resolve identified shortcomings, giving priority to the most significant issues so they can be corrected as quickly as possible. We are committed to reducing risks to the agency's systems and information and to successfully responding to the findings and recommendations set forth in the report.

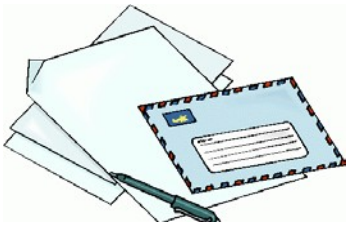
CONTACT US

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

Call:
Inspector General's HOTLINE: 301-504-7906
Or: 1-866-230-6229

Click here for complaint form.

Click here for CPSC OIG website.



Or Write:

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