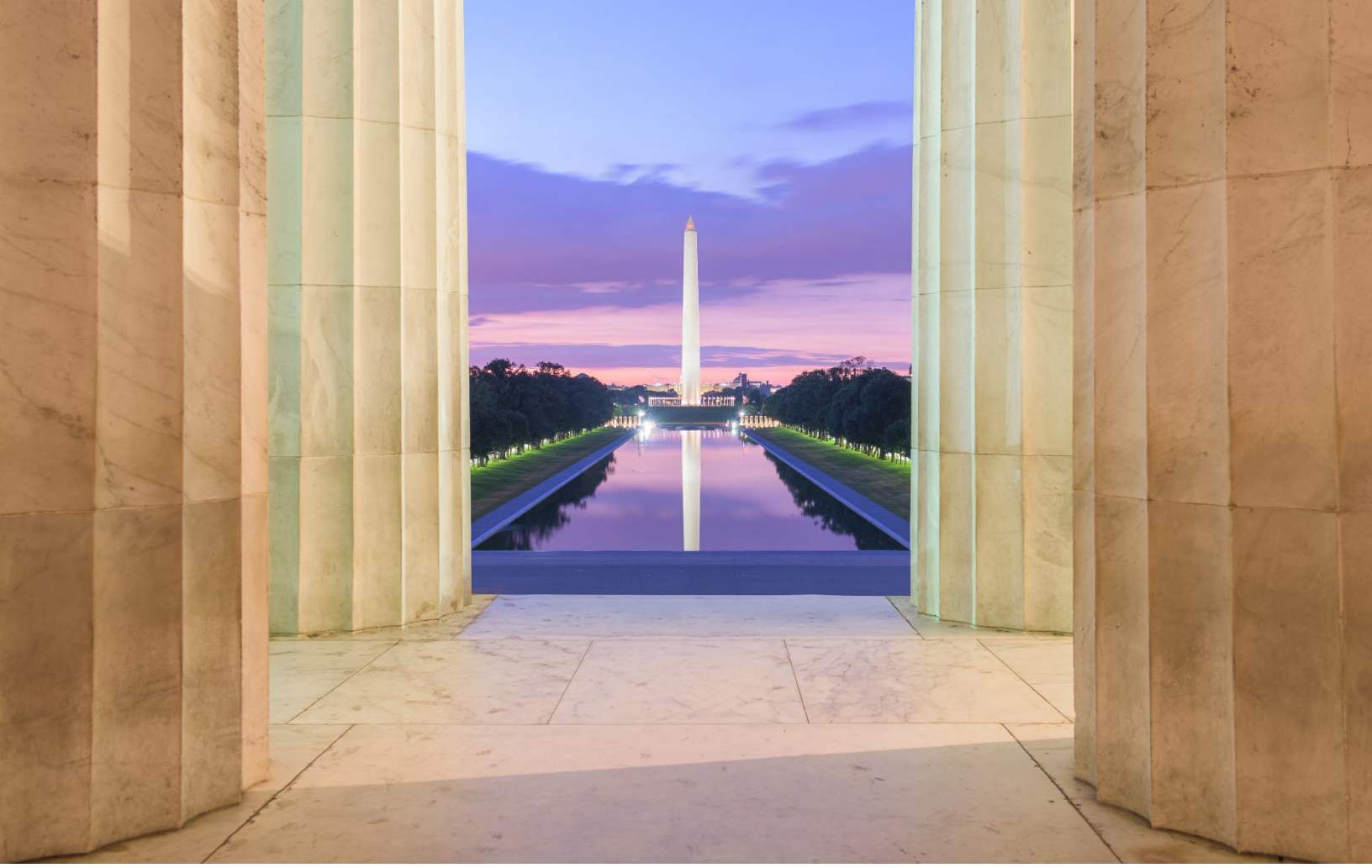
U.S. Consumer Product Safety Commission
OFFICE OF INSPECTOR GENERAL

CPSC Penetration Test 2022

December 13, 2022

23-A-02



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.

December 13, 2022

TO: Alexander Hoehn-Saric, Chairman
Peter A. Feldman, Commissioner
Richard Trumka Jr., Commissioner
Mary T. Boyle, Commissioner

FROM: Christopher W. Dentel, Inspector General

Christopher W. Dentel

Digitally signed by Christopher W. Dentel
Date: 2022.12.13 08:55:48 -05'00'

SUBJECT: CPSC Penetration Test 2022

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 Williams, Adley & CO.-DC LLP (Williams Adley), an independent public accounting firm. Under a contract monitored by the OIG, Williams Adley engaged a subcontractor, Cerberus Cyber Sentinel Corporation (Cerberus), to perform an IT security assessment known as a Penetration Test. The CPSC insisted that certain key IT systems not be assessed. This limited the value of the assessment immensely, as the areas with the greatest likelihood to have a significant impact on agency operations (and therefore, the most important targets to assess) were excluded from the assessment.

The contract required that the assessment be performed in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation (CIGIE QSIE). We reviewed the resulting report and related documentation and made relevant inquires to the contractors. Our review was not intended to enable us to express, and we do not express, an opinion on the matters contained in the report. Williams Adley is responsible for the attached report. However, our review disclosed no instances where either Williams Adley or Cerberus did not comply, in all material respects, with CIGIE's QSIE.

Cerberus assessed the security of the CPSC's IT infrastructure by first conducting reconnaissance and gathering intelligence on the CPSC and CPSC users, then performing target discovery (e.g. network discovery, network port and service identification, etc.). They then identified and cataloged the security flaws. Their work should assist the CPSC in identifying security weaknesses that, if exploited, could have a significant negative impact on the confidentiality, integrity, and availability of agency information systems and data. Cerberus made 14 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.

EXECUTIVE SUMMARY

CPSC Penetration Test 2022

December 13, 2022

BACKGROUND The U.S. Consumer Product Safety Commission (CPSC) Office of Inspector General (OIG) retained the services of Williams, Adley & CO.-DC LLP (Williams Adley), an independent public accounting firm. Under a contract monitored by the OIG, Williams Adley engaged a subcontractor, Cerberus Cyber Sentinel Corporation (Cerberus or we), to perform a security assessment, known as a penetration test, on select CPSC systems. Cerberus is a nationwide provider of cybersecurity consulting and managed services, with offices and resources all across the U.S. and is a publicly traded company.

Under the Federal Information Security Modernization Act of 2014, the Office of Management and Budget directed the National Institute of Standards and Technology (NIST) to develop guidance for federal agencies to test and assess the security of their information systems. NIST Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment*, provides this guidance. Cerberus used this guidance in addition to its knowledge of industry best practices to perform this assessment.

Penetration testing mimics real-world attacks to identify methods for circumventing the security features of an application, system, or network. As discussed in the Scope Limitation section, the CPSC insisted that certain significant information technology systems not be subject to testing.

OBJECTIVE The penetration test was designed to assess the information security posture of the CPSC applications and systems from both an external and internal perspective to determine risks posed from unauthorized users. The objective of this assessment was to identify security issues, and more importantly, to put those security issues in context.

All identified security controls and weaknesses were evaluated holistically to demonstrate the potential impact on the environment if exploited, so that the organization may target tactical and strategic initiatives where the need is most acute. Cerberus also documented (1) the threats posed that would effect the likelihood that a vulnerability would be exploited, (2) any criteria, guidance, and best practices related to the security weakness, and (3) the root cause of the security weakness.

ASSESSMENT We performed both an external penetration test and a limited internal penetration test. We identified three high risk vulnerabilities, two medium risk vulnerabilities, and eight low risk vulnerabilities as a result of this assessment.

The first phase of the assessment was an external penetration test (i.e., a "black-box penetration test") meaning we had no prior knowledge of the CPSC's network operations or configurations, and we were not given a foothold on the CPSC's internal

Report addresses CPSC's Cross Cutting Priority #2: Information technology
OIG's Management Challenges #4: Information Technology Security

EXECUTIVE SUMMARY

network or granted "authorized" access to the agency's physical space.

During this phase of our assessment, we identified one high risk vulnerability and six low risk vulnerabilities. For example, we noted that the CPSC has sensitive data exposed on its website. We also identified missing security features of the targeted web applications. Finally, we demonstrated that we were able to gain access to CPSC systems.

The next phase of the assessment was a limited internal penetration test (i.e., a "grey-box penetration test"), meaning we were given a foothold in the CPSC's network, but were not provided with credentials or knowledge of the network/system configurations.

As part of our internal assessment, we identified two high risk, two medium risk, and two low risk vulnerabilities. For example, we were able to capture, enumerate, and crack password hashes, in addition to other, less serious weaknesses that require attention.

SCOPE LIMITATION

Management identified large areas which were not to be subject to testing in the rules of engagement that all parties signed at the start of this assessment. Management stated that they wished to prevent the "potential for the significant disruption of agency operations." Thus we are unable to opine on the security of those areas. This limited the value of the assessment immensely, however, as the areas with the greatest likelihood to have a significant impact on agency operations (and therefore, the most important targets to assess) were excluded from scope.

We recommend testing the excluded areas in the near future to identify the risks they pose to the CPSC and its mission. Currently, this risk is unknown.

AGENCY RESPONSE

We shared the results of this assessment with CPSC senior management and Office of Information & Technology Services staff during the engagement and at a meeting on December 13, 2022. Management generally concurred with our findings and recommendations.

RECOMMENDATIONS

We made 14 actionable recommendations to the CPSC. The full CPSC Penetration Test 2022 report shared with CPSC management contains the details of the observations we made during testing. It also contains supporting data and our analysis of the threat and potential impact of the security weaknesses within the context of the CPSC's environment.

For more information on this report please contact us at CPSC-OIG@cpsc.gov

To report fraud, waste, or abuse, mismanagement, or wrongdoing at the CPSC go to OIG.CPSC.GOV or call (301) 504-7906

Office of Inspector General, CPSC, 4330 East-West Hwy., Suite 702, Bethesda, MD. 20814