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

Evaluation of the CPSC's NIST Cybersecurity Framework Implementation

January 18, 2022

22-A-04

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.

January 18, 2022

TO: Alexander Hoehn-Saric, Chair
Dana Baiocco, Commissioner
Peter A. Feldman, Commissioner
Richard L. Trumka Jr., Commissioner

FROM: Christopher W. Dentel, Inspector General Christopher W. Dentel Digitally signed by Christopher W. Dentel Date: 2022.01.18 08:59:13 -05'00'

SUBJECT: Evaluation of the CPSC's NIST Cybersecurity Framework Implementation

This report evaluates the U.S. Consumer Product Safety Commission's (CPSC) progress in implementing the National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity* (CSF). The CSF provides guidelines for organizations to evaluate and improve an agency's cybersecurity posture. This approach requires management to consider cybersecurity risks as part of the organization's overall risk management assessment, specifically with a focus on an agency's cybersecurity risk. The Office of Inspector General retained the services of Williams Adley & Company –DC LLP (Williams Adley), an independent public accounting firm, to assess the CPSC's implementation of NIST's CSF. This evaluation was performed in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation (CIGIE QSIE).

Williams Adley determined that the CPSC has not implemented the CSF. Williams Adley made five recommendations to aid the CPSC as it implements the CSF which will allow agency staff to provide reliable and secure information systems to meet its mission and keep the American people safe. In connection with our contract, we reviewed Williams Adley'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. Williams Adley is responsible for the attached report. However, our review disclosed no instances where Williams Adley did not comply, in all material respects, with CIGIE's QSIE.

In the next 30 calendar days, in accordance with Office of Management and Budget Circular A-50, the CPSC is required to provide me with management's Corrective Action Plan describing the specific actions they anticipate taking to implement each recommendation. Should you have any questions, please contact me.

Table of Contents

Executive Summary

Citizens rely on the U.S. Consumer Product Safety Commission (CPSC) to keep them safe, and the CPSC relies on information systems to meet its mission. Today's cybersecurity threats exploit the increased complexity and connectivity of critical information systems placing the nation's security, economy, and public safety and health at risk. Similar to financial and reputational risks, cybersecurity risk affects an agency's operations and ability to meet its mission. Further, it can harm an agency's ability to innovate and to meet future challenges.

Federal agencies are required to implement the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) to minimize their cybersecurity risks and to increase the protection of critical information systems. The NIST CSF focuses on using business drivers to guide cybersecurity activities by considering cybersecurity risks as part of an organization's overall risk management processes. In order to implement the NIST CSF, agencies must take specific actions to design, implement, and evaluate how the agency will leverage the NIST CSF to support their agency's cybersecurity program.

The CPSC Office of Inspector General retained Williams Adley, & Co.-DC LLP (Williams Adley), an independent public accounting firm, to perform an independent evaluation of the CPSC's implementation of the NIST CSF. This report documents the results of the NIST CSF evaluation.

What We Found

Overall, based on the evaluation procedures performed, Williams Adley has determined that the CPSC has not implemented the NIST CSF in accordance with requirements.

What We Recommend

To improve the CPSC's implementation of the NIST CSF, we made five recommendations that the CPSC must address to improve its cybersecurity posture.

1. OBJECTIVE

The objective of this effort was to perform an independent evaluation of the CPSC's implementation of the NIST CSF.

2. BACKGROUND

Cybersecurity Framework

In response to the growing concern related to cybersecurity, Executive Order 13636[1] was issued which required the development of a set of cybersecurity standards and best practices to help organizations manage cybersecurity risks to agency operations and its mission. As a result of this Executive Order, NIST released the *Framework for Improving Critical Infrastructure Cybersecurity* [*Cybersecurity Framework*] on February 12, 2014. The NIST CSF[2] provides guidelines for organizations to evaluate and improve the agency's cybersecurity risk. This approach requires management to consider cybersecurity risks as part of the organization's overall risk management processes.

To further emphasize the importance of protecting federal networks, Executive Order 13800[3] was issued to improve the nation's cybersecurity posture and capabilities. Specifically, Executive Order 13800 requires agency heads to lead integrated teams of senior executives with expertise in information technology, security, budgeting, acquisition, law, privacy, and human resources. Furthermore, Executive Order 13800 requires agency heads to use the NIST CSF to manage the agency's cybersecurity risk. Additionally, it holds agency heads accountable for ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes. This order required agencies to report to the Office of Management and Budget (OMB) on how they planned to implement the NIST CSF by August 15, 2017.[4]

[1] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013.
[2] This was updated by the publication of Version 1.1 of the Cybersecurity Framework in April, 2018.
[3] Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 11, 2017.
[4] Executive Order 13800, stated "Each agency head shall provide a risk management report to the Secretary of Homeland Security and the Director of the OMB within 90 days [August 15, 2017] of the date of this order" and "describe the agency's action plan to implement the Framework".

Implementing the Cybersecurity Framework

Federal Information Security Modernization Act (FISMA) requires federal agencies to develop, document, and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency. Furthermore, FISMA "emphasizes a risk-based policy for cost-effective security," underscoring the importance of agencies taking a risk-based approach to protecting their information and information systems and addressing their unique cybersecurity challenges. The CSF provides management with a structure to prioritize tasks necessary to implement FISMA. Initial implementation of the NIST CSF requires agencies to complete and document the seven actions listed below.[5]

1. Prioritize and Scope: The agency must identify its business and mission objectives and high-level organizational priorities.

2. Orient: The agency must identify related information systems and assets, regulatory requirements, the overall agency risk approach, and the threats and vulnerabilities applicable to those information systems and assets.

3. Create a Current Profile: The agency must develop a current profile (i.e., identify the cybersecurity control areas and techniques currently implemented at the agency).

4. Conduct a Risk Assessment: The agency must analyze the operational environment to discern the likelihood of a cybersecurity event and the impact that event could have on the agency.

5. Create a Target Profile: The agency must create a target profile that focuses on the assessment of the NIST CSF categories and subcategories describing the agency's desired cybersecurity outcome.

6. Determine, Analyze, and Prioritize Gaps: The agency must compare the current profile and the target profile to identify gaps and create a prioritized action plan to address gaps.

7. Implement Action Plan: The agency must determine which actions to take to address the gaps, if any, identified in the previous step, and then adjust its current cybersecurity practices to achieve the target profile.

The five functions (identify, protect, detect, respond, and recover) of the NIST CSF rubrics provide agencies with the structure and guidance to improve their information security program by using an effective risk management strategy to manage and protect their environment. These functions require that organizations make use of risk management processes to inform and prioritize decisions regarding information security. The five functions support recurring risk assessments and the

[5] Version 1.1 of the Cybersecurity Framework was published in April, 2018 to provide refinements, clarifications, and enhancements to Version 1.0, Section 3.1, published in February, 2014.

validation of business drivers to help agencies prioritize and implement the necessary information security activities that reflect desired outcomes. Each function places reliance on the development of those preceding it. For example, an organization cannot **protect** its information technology environment effectively without first **identifying** its key information systems and the risks faced by each. Moreover, an organization cannot **respond** to cybersecurity events if it has not first implemented proper measures to **detect** them. The below image gives a high-level overview of the activities associated with each function.

Image 1: NIST CSF Functions and Lifecycle.

3. FINDING: The CPSC Has Not Implemented the NIST CSF

Overall, based on the evaluation procedures performed, Williams Adley has determined that the CPSC has not implemented the NIST CSF in accordance with requirements. Each of the related conditions are documented below.

Cybersecurity Framework Conditions

The CPSC Office of Information Technology (EXIT) is responsible for implementing the NIST CSF and related practices in support of their responsibility for implementing the agency's cybersecurity program. EXIT originally generated a high-level action plan and timely submitted this plan to OMB in 2017, however, the action plan was not implemented. Williams Adley noted that EXIT has not:

- defined a NIST CSF current profile
- completed a risk assessment that identified, measured, and assigned values to potential cybersecurity risks to determine if the CPSC has considered the costs and benefits of reducing cybersecurity risks
- completed a NIST CSF target profile
- performed an assessment to identify current state and target state gaps and used this analysis to update its NIST CSF Action Plan
- implemented a NIST CSF Action Plan

Cause

The CPSC did not complete the actions as prescribed by the NIST CSF, and as documented in their original action plan, because the CPSC focused their resources on other priorities. The CPSC asserts that it did not complete this because the CPSC focused its limited resources on addressing an unprecedented number of Department of Homeland Security Emergency Directives, Binding Operational Directives, critical security advisories, and cyber threats during the period in question.

Effect

By not implementing the NIST CSF, the CPSC missed a powerful opportunity to leverage government and industry best practices when prioritizing cybersecurity efforts, thus increasing the ongoing cybersecurity risk to its mission to keep consumers safe.

Recommendations

Below we have provided a list of recommendations that the CPSC must implement to meet NIST CSF requirements.

1. Complete a National Institute of Standards and Technology (NIST) Cybersecurity Framework current profile in accordance with NIST guidance.

2. Conduct an assessment to identify the highest risks to the CPSC's security profile based on the information learned while completing the National Institute of Standards and Technology Cybersecurity Framework current profile exercise.
3. Complete a National Institute of Standards and Technology (NIST) Cybersecurity Framework target profile in accordance with NIST guidance.
4. Perform an assessment to identify gaps between the current and target National Institute of Standards and Technology Cybersecurity Framework profiles.
5. Update and implement the CPSC Framework Implementation Action Plan.

4. CONSOLIDATED LIST OF RECOMMENDATIONS

Table 4-1: Index of Recommendations

Finding	Recommendation
Cybersecurity Framework	1. Complete a National Institute of Standards and Technology (NIST) Cybersecurity Framework current profile in accordance with NIST guidance. 2. Conduct an assessment to identify the highest risks to the CPSC's security profile based on the information learned while completing the National Institute of Standards and Technology Cybersecurity Framework current profile exercise. 3. Complete a National Institute of Standards and Technology Cybersecurity Framework (NIST) target profile in accordance with NIST guidance. 4. Perform an assessment to identify gaps between the current and target National Institute of Standards and Technology Cybersecurity Framework profiles. 5. Update and implement the CPSC Framework Implementation Action Plan.

Appendix A. Objective, Scope, and Methodology

A.1 Objective & Scope

The objective of the NIST CSF evaluation is to determine the status of CPSC's implementation of the NIST CSF. The evaluation covered the period of October 1, 2020, to September 30, 2021.

A.2 Methodology

Williams Adley performed this evaluation from April through October 2021 and conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency *Quality Standards for Inspections and Evaluations*. Those standards require that Williams Adley obtain sufficient evidence to provide a reasonable basis for their findings and conclusions based on their objectives.

To perform this evaluation, Williams Adley interviewed CPSC key personnel and reviewed supporting documentation to determine the status of the CPSC implementation of NIST CSF requirements.

Assessment, testing, and analysis were performed in accordance with guidance from the following:

- Executive Order 13636, *Improving Critical Infrastructure Cybersecurity,* February 12, 2013
- Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 11, 2017
- NIST Cybersecurity Framework, Version 1.1, *Framework for Improving Critical Infrastructure Cybersecurity*, April 16, 2018
- NIST Interagency Report 8170, *Approaches for Federal Agencies to Use the Cybersecurity Framework*, March, 2020

Appendix B. Management Response

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

Memorandum

Date: January 7, 2022

TO : Christopher Dentel
Inspector General
Office of the Inspector General

FROM : James Rolfes
Chief Information Officer
Office of Information and Technology Service

SUBJECT : Management Response to Evaluation of the CPSC's NIST CSF Implementation

In response to the *Fiscal Year 2021 CPSC NIST CSF Implementation Evaluation*, Management generally concurs with the report's findings and recommendations and acknowledges that the findings and recommendations are important to the protection of agency systems and information. CPSC will establish plans to address the recommendations identified in the evaluation.

CPSC takes cybersecurity seriously and works diligently to respond to emerging threats, address vulnerabilities and incorporate it into ongoing program improvements, system modernization, data management, and cloud migration activities to reduce agency risk.

CC:
Mary Boyle, Executive Director
DeWane Ray, Deputy Executive Director for Operations
Patrick Manley, Chief Information Security Officer

Appendix C. Acronyms

CPSC	U.S. Consumer Product Safety Commission
CSF	Cybersecurity Framework
EXIT	Office of Information and Technology Services
FISMA	Federal Information Security Modernization Act
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
Williams Adley	Williams, Adley, & Co.-DC LLP

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