Office of Inspector General
Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

Executive Summary, 2020-IT-C-021, November 2, 2020

2020 Audit of the Bureau's Information Security Program

Findings

The Bureau of Consumer Financial Protection's information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity. For instance, the Bureau's information security continuous monitoring process is effective; the agency integrated metrics on the effectiveness of its process across the organization. Further, the Bureau's incident response process is similarly effective; the agency implemented a new incident ticket system that is more closely integrated with configuration management activities.

Similar to previous years, we identified opportunities for the Bureau to strengthen its information security program in Federal Information Security Modernization Act of 2014 (FISMA) domains across all five National Institute of Standards and Technology Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective. This year, we identified policy and technology improvements needed to strengthen separation of duties controls in the Bureau's configuration management processes.

We also found that the Bureau has taken sufficient actions to close 4 of the 14 recommendations from our prior FISMA audits that were open at the start of this audit. These 4 recommendations are related to risk management, identity and access management, and incident response. The remaining 10 recommendations, related to risk management, configuration management, identity and access management, data protection and privacy, incident response, and contingency planning, remain open. We will continue to monitor the Bureau's progress in these areas as part of our future FISMA reviews

Recommendation

This report includes one new recommendation designed to strengthen the Bureau's information security program in the area of configuration management. In its response to a draft of our report, the Bureau concurs with our recommendation and outlines actions that have been or will be taken to address it. We will continue to monitor the Bureau's progress in addressing this recommendation as part of future FISMA audits.

Purpose

To meet our annual FISMA reporting responsibilities, we reviewed the information security program and practices of the Bureau. Our specific audit objectives, based on the legislation's requirements, were to evaluate the effectiveness of the Bureau's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices.

Background

FISMA requires each inspector general to conduct an annual independent evaluation of its agency's information security program, practices, and controls for select systems. The U.S. Department of Homeland Security's guidance for FISMA reporting directs inspectors general to evaluate the maturity level (from a low of 1 to a high of 5) of their agencies' information security programs across several areas. The guidance notes that level 4 (*managed and measurable*) represents an effective level of security.