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

Executive Summary, 2021-IT-C-015, October 29, 2021

2021 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. Since our review last year, we found that the Bureau has taken several steps to strengthen its information security program. For instance, the agency has leveraged its information security training skills assessment to identify improvements needed in staffing levels. Further, the Bureau continues to capture and report incident response metrics and is evaluating the use of automation to strengthen ticketing processes.

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. Specifically, we identified opportunities to improve the Bureau's organizationwide cybersecurity risk management processes through the use of a cybersecurity risk register process. We also found that the Bureau was not ensuring that specific technical vulnerabilities were appropriately tracked in a plan of actions and milestones. In addition, we found that the Bureau had not updated its configuration management plan to reflect new technologies and processes.

In addition, the Bureau has taken sufficient actions to close 2 of the 11 recommendations from our prior FISMA audit reports that were open at the start of this audit. The closed recommendations relate to the implementation of mobile device management technologies and completion of a business impact analysis for information technology systems. We are leaving open 9 recommendations related to risk management, configuration management, data protection and privacy, and identity and access management. We will update the status of these recommendations in our spring 2022 semiannual report to Congress and continue to monitor the Bureau's progress as part of future FISMA audits.

Recommendations

This report includes three new recommendations designed to strengthen the Bureau's information security program in the areas of risk and configuration management. In its response to a draft of our report, the Bureau concurs with our recommendations and outlines actions that have been or will be taken to address them. We will continue to monitor the Bureau's progress in addressing these recommendations 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.