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

Executive Summary, 2019-IT-C-015, October 31, 2019

2019 Audit of the Bureau's Information Security Program

Findings

Since our review last year, the Bureau of Consumer Financial Protection (Bureau) has matured its information security program. Specifically, we found that the Bureau's information security program is operating effectively at a level-4 (*managed and measurable*) maturity. For instance, the Bureau's information security continuous monitoring process is effective, with the agency enhancing the functionality of its security information and event-monitoring tool. Further, the Bureau's incident response process is similarly effective, with the agency using multiple tools to detect and analyze incidents and track performance metrics.

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 Cybersecurity Framework security functions—*identify, protect, detect, respond,* and *recover*—to ensure that its program remains effective. Specifically, as we noted last year, the agency can strengthen its enterprise risk management program by defining a risk appetite statement and associated risk tolerance levels. Further, the Bureau has not identified its high-value assets and determined what governance and security program changes may be needed to effectively manage security for those assets. Additionally, we identified improvements needed in the implementation of the Bureau's security assessment and authorization processes to manage security risks prior to deploying Bureau systems. We also identified improvements needed in database security, timely remediation of vulnerabilities, and patching of mobile phone operating systems.

Finally, the Bureau has taken sufficient action to close 3 of the 10 recommendations from our prior FISMA audits that remained open at the start of this audit. The closed recommendations relate to data protection and privacy, incident response, and contingency planning. We are leaving open 7 recommendations in the areas of risk management, configuration management, and identity and access management. We will continue to monitor the Bureau's progress in these areas as part of future FISMA reviews.

Recommendations

This report includes 7 new recommendations designed to strengthen the Bureau's information security program in the areas of risk management, identity and access management, data protection and privacy, incident response, and contingency planning. 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 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. U.S. Department of Homeland Security 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.