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

Executive Summary, 2018-IT-C-018, October 31, 2018

2018 Audit of the Bureau’s Information Security Program

Findings

The Bureau of Consumer Financial Protection’s (Bureau) information security program is operating at a level-3 (*consistently implemented*) maturity, with the agency performing several activities indicative of a higher maturity level. For instance, the Bureau’s information security continuous monitoring process is effective and operating at level 4 (*managed and measurable*), with the agency reporting on performance measures related to supporting activities. Further, the Bureau’s incident response process is similarly effective, with the agency using tools to detect and analyze incidents and track performance metrics.

The Bureau also has opportunities to mature 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 is 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. The Bureau can also improve its processes related to database security, timely remediation of vulnerabilities, and patching of mobile phone operating systems. Further, access to one of the Bureau’s internal collaboration tools, which contains sensitive information (including personally identifiable information), was not restricted to individuals with a need to know.

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 identity and access management, incident response, and contingency planning. We will continue to monitor the Bureau’s progress as part of future FISMA reviews.

Recommendations

This report includes 4 new recommendations designed to strengthen the Bureau’s information security program in the areas of configuration management, identity and access management, and data protection and privacy. In response to a draft of our report, the Chief Information Officer 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 agency’s information security program across several areas. The guidance notes that level 4 (*managed and measurable*) represents an effective level of security.