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

Executive Summary, 2018-IT-B-017, October 31, 2018

2018 Audit of the Board's Information Security Program

Findings

The Board of Governors of the Federal Reserve System's (Board) information security program is operating at a level-4 (*managed and measurable*) maturity, which indicates an overall effective level of security. For instance, the Board has enhanced its identity and access management program by requiring multifactor authentication for access to its network for all privileged and nonprivileged users. Further, the agency has implemented an effective security training program that includes phishing exercises and associated performance metrics.

The Board also has opportunities to mature its information security program in Federal Information Security Modernization Act of 2014 (FISMA) domains across all five security functions outlined in the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective. Similar to our 2017 audit, a consistent theme we noted is that the lack of an agencywide risk management governance structure and strategy, as well as the decentralization of information technology services, results in an incomplete view of the risks affecting the Board's security posture. Although the Board has taken steps to move toward an agencywide approach to risk management governance and information technology services, several security processes, such as asset management and enterprise architecture, have not yet been implemented agencywide.

Finally, the Board has taken sufficient action to close 4 of the 13 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 are leaving open 9 recommendations in the areas of risk management, configuration management, identity and access management, and information security continuous monitoring from our 2016 and 2017 FISMA audits. We will continue to monitor the Board's progress as part of future FISMA reviews.

Recommendations

This report includes six new recommendations designed to strengthen the Board's information security program in the areas of risk management, configuration management, data protection and privacy, and security training. In her response to our draft report, the Board's Chief Information Officer concurs with our recommendations and notes actions that are underway to strengthen the Board's information security program. We will continue to monitor the Board's progress on 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 Board. Our specific audit objectives, based on the legislation's requirements, were to evaluate the effectiveness of the Board'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.