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

Executive Summary, 2017-IT-B-018, October 31, 2017

2017 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-3 (*consistently implemented*) maturity, with the agency performing several activities indicative of a higher maturity level. For instance, the Board has enhanced its configuration management practices to more effectively detect unauthorized hardware and software on its network. Further, it 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 to ensure that it is effective. 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 security posture of the Board and impedes its ability to implement an effective information security program. We also found that several security processes, such as configuration management and information security continuous monitoring, were not effectively implemented agencywide.

Finally, the Board has taken sufficient action to close 6 of the 10 recommendations from our prior Federal Information Security Modernization Act of 2014 (FISMA) audits that remained open at the start of this audit. Efforts to address the remaining recommendations are underway, and we will continue to monitor the Board's progress as part of our future FISMA audits.

Recommendations

Our report includes nine new recommendations designed to strengthen the Board's information security program in the areas of risk management, configuration management, identity and access management, information security continuous monitoring, and contingency planning. In its response to our draft, the Board concurs with our recommendations and notes that actions are underway to strengthen the Board's information security program. We will continue to monitor the Board'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 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 agencies' information security programs across several areas. The guidance notes that level 4 (*managed and measurable*) represents an effective level of security.