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

Executive Summary, 2019-IT-B-016, October 31, 2019

2019 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 effectively at a level-4 (*managed and measurable*) maturity. For instance, the Board has implemented its new suitability policy and assigned personnel risk designations to all Board positions. In addition, the Board has implemented automated mechanisms to more effectively support account management processes for privileged users across the organization.

The Board 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 remains effective. Similar to our previous FISMA audits, a consistent theme we noted is that the decentralization of information technology services results in an incomplete view of the risks affecting the Board's security posture. In addition, the Board has not defined its enterprisewide risk management strategy, risk appetite, and risk tolerance levels, which could help guide cybersecurity processes across function areas. While the Board has taken steps to move toward an enterprisewide approach to the delivery of information technology services and risk management, 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 3 of the 15 recommendations from our prior FISMA audits that remained open at the start of this audit. The closed recommendations relate to configuration management, identity and access management, and data protection and privacy. We are leaving open 12 recommendations in the areas of risk management, configuration management, identity and access management, data protection and privacy, security training, and information security continuous monitoring from our 2016, 2017, and 2018 FISMA audits. We will update the status of these recommendations in our upcoming semiannual report to Congress and continue to monitor the Board's progress as part of future FISMA reviews.

Recommendations

This report includes 6 new recommendations designed to strengthen the Board's information security program in the areas of risk management, identity and access management, and data protection and privacy. In its response to a draft of our report, 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 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.