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

Executive Summary, 2020-IT-B-020, November 2, 2020

2020 Audit of the Board’s Information Security Program

Findings

The Board of Governors of the Federal Reserve System’s information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity. The Board continues to take steps to strengthen its information security program. For instance, the Board has finalized its *Vendor Risk Management Standard* and updated the information security clauses in its standard contracting language. In addition, the Board has implemented several role-based training offerings for individuals with significant security responsibilities, including application developers, system owners, and authorizing officials.

The Board has opportunities to mature its information security program in Federal Information Security Modernization Act of 2014 (FISMA) domains across all five National Institute of Standards and Technology 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 completed defining its enterprisewide risk management strategy, risk appetite, and risk tolerance levels, which could help guide cybersecurity processes across function areas. We also believe that the Board’s ongoing efforts to implement the U.S. Department of Homeland Security’s Continuous Diagnostic and Mitigation program will continue to mature the agency’s information security program across multiple security functions and help address issues that result from the decentralization of information technology services.

Finally, the Board has taken sufficient actions to close 7 of the 18 recommendations from our prior FISMA audits that remained open at the start of this audit. 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 4 new recommendations and 2 items for management’s consideration designed to strengthen the Board’s information security program in the areas of risk management, configuration management, identity and access management, data protection and privacy, and information security continuous monitoring. 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 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 their agency’s information security program, practices, and controls for select systems. The U.S. Department of Homeland Security’s 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.