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

Executive Summary, 2024-IT-B-020, October 31, 2024

2024 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. We found that the Board has taken steps to strengthen its information security program since our 2023 Federal Information Security Modernization Act of 2014 (FISMA) audit report. For instance, the Board has updated its personnel security processes to help ensure position risk designations are documented and used in personnel security processes. However, we identified several areas in which the Board's information security program decreased in maturity from prior years.

To ensure that its information security program remains effective, the Board should

- develop a supply chain risk management strategy
- define a review and escalation process for alerts generated by the Board's data loss prevention tool
- consistently document system interconnections and required documentation
- perform vulnerability scanning on mobile devices and applications
- annually test, review, and approve the incident notification and breach response plan to maintain organizational cyber resiliency
- provide role-based privacy training to help ensure that individuals are knowledgeable and aware of their privacy roles and responsibilities
- perform targeted phishing exercises to increase the cyber awareness of the Board's executives and those with significant security responsibilities
- ensure that contractual requirements for the Board's cloud service providers for the timely reporting of incidents are consistent with federal requirements

Finally, 14 recommendations that we made in our prior FISMA audit reports remain open. We will continue to monitor the Board's progress in addressing these recommendations as part of future FISMA audits. We believe that if sufficient progress is not made to address our prior open recommendations as well as the 9 new recommendations in this report, the Board's information security program maturity rating could decline in 2025.

Recommendations

This report includes nine new recommendations designed to strengthen the Board's information security program in the areas of risk management, supply chain risk management, data protection and privacy, and security training. In its response to a draft of our report, the Board concurs with our recommendations and plans to provide us with plans of action and milestones to address each recommendation. We will monitor the Board's progress in addressing these recommendations as part of future FISMA 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 selected information systems and (2) information security policies, procedures, standards, and guidelines.

Background

FISMA requires each inspector general to conduct an annual independent evaluation of their agency's information security program, practices, and controls for selected systems. The Office of Management and Budget's (OMB) *FY 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* 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 for fiscal year 2024. OMB notes that level 4 (*managed and measurable*) represents an effective level of security.