Office of Inspector General

Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

Executive Summary, 2023-IT-B-015, September 29, 2023

2023 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. Since our review last year, we found that the Board has taken steps to strengthen its information security program. For instance, the Board has expanded the coverage of its vulnerability disclosure program to include all internet-accessible systems. In addition, the Board has strengthened its supply chain risk management program through improved documentation of its processes.

We identified five new findings to strengthen the Board's information security program in the *identify* and *protect* function areas. Specifically, we found that the Board has not defined the organization's cybersecurity risk tolerance and that the agency's cybersecurity risk register is missing required information. In addition, the Board has not defined its process for consistently inventorying and documenting necessary attributes for its web applications or third-party systems. Further, the Board can strengthen mobile device security by ensuring that mobile device operating systems are updated timely and by denying access to enterprise services when they are not. Lastly, we found that the majority of the Board's privacy impact assessments are not updated and reviewed in accordance with the agency's policy.

Finally, seven recommendations we made in our previous Federal Information Security Modernization Act of 2014 (FISMA) audit reports remain open. These recommendations relate to risk management, identity and access management, data protection and privacy, security training, and information security continuous monitoring.

Recommendations

This report includes seven new recommendations designed to strengthen the Board's information security program in the *identify* and *protect* function areas. In its response to a draft of our report, the Board concurs with our recommendations and outlines actions 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 select 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 2023. OMB notes that level 4 (*managed and measurable*) represents an effective level of security.