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

Executive Summary, 2025-IT-B-011R, October 31, 2025

2025 Audit of the Board's Information Security Program

Findings

The Board's information security program has decreased from a level-4 maturity (*managed and measurable*) in fiscal year (FY) 2024 to a level-3 maturity *(consistently implemented)* in FY 2025. We further concluded, based on the results of our determinations of effectiveness in each domain and function, that the Board's overall information security program is not effective. We found that the Board has taken some steps to strengthen its information security program since our 2024 Federal Information Security Modernization Act of 2014 (FISMA) audit report. For instance, the Board has updated its cybersecurity risk register process and developed a new information security continuous monitoring strategy. However, challenges in cybersecurity governance resulting from the Board's information technology (IT) operating model and decentralized IT environment, coupled with opportunities to strengthen foundational cybersecurity elements, contributed to the decline in overall program maturity.

We found that the Board can strengthen its cybersecurity program by

- defining key elements of its current and target cybersecurity approach
- reassessing its policy for mobile device use and consistently enforcing mobile content and data protection controls
- reassessing the feasibility of developing and implementing an information classification for confidential supervisory information

Recommendations

This report includes three new recommendations and a matter for management consideration designed to strengthen the Board's information security program in the areas of cybersecurity governance, mobile device security, and confidential supervisory information protection. In its response to our draft report, the Board concurs with our recommendations and outlines actions to address each recommendation. We will follow up to ensure that the recommendations are fully addressed.

In addition, we are closing 4 previously issued recommendations, while keeping 18 recommendations made in our prior FISMA reports open. Notably, the Board has not yet addressed several significant recommendations related to insider threat management, data loss prevention, and cyber risk tolerance. We will continue to monitor the Board's progress in addressing these recommendations as part of future FISMA audits. Given the sensitivity of the information in our review, portions of the public version of this report have been redacted.

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 2025 Inspector General 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 FY 2025. OMB notes that level 4 *(managed and measurable)* represents an effective level of security.

A key addition in the *FY 2025 Inspector General FISMA Reporting Metrics* is the inclusion of a new *govern* function that focuses on the role governance plays in managing cybersecurity risks and incorporating cybersecurity into an organization's broader enterprise risk management strategy.