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

Executive Summary, 2022-IT-B-013, September 30, 2022

# 2022 Audit of the Board’s Information Security Program

## Finding

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 developed a strategy for the implementation of a zero trust architecture (ZTA), in accordance with Executive Order 14028, *Improving the Nation’s Cybersecurity*. In support of its ZTA strategy, the Board has launched an organizationwide multifactor authentication effort and engaged with an external consultant to perform a ZTA maturity assessment for the agency. Further, the Board has continued to implement the U.S. Department of Homeland Security’s Continuous Diagnostics and Mitigation program, which provides cybersecurity tools, integration services, and dashboards to participating agencies to help them improve their security posture.

We identified opportunities to strengthen the Board’s cybersecurity risk management processes. Specifically, we found that the Board could strengthen its cybersecurity risk register process by categorizing and prioritizing risks. We also found that the questionnaire the Board uses to assess the information security posture of potential vendors could be updated to include specific questions related to (1) the protection of information at rest and (2) software, firmware, and information integrity.

Finally, the Board has taken sufficient actions to close three of the nine recommendations from our prior Federal Information Security Modernization Act of 2014 (FISMA) audit reports that remained open at the start of this audit. The closed recommendations are related to risk management. We are leaving open six recommendations related to risk management, identity and access management, data protection and privacy, security training, and information security continuous monitoring. We will update the status of these recommendations in our fall 2022 semiannual report to Congress and continue to monitor the Board’s progress as part of future FISMA audits.

## Recommendation

This report includes one new recommendation and one matter for management consideration designed to strengthen the Board’s information security program in the area of cybersecurity risk management. In its response to a draft of our report, the Board concurs with our recommendation. We will monitor the Board’s progress in addressing this recommendation 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 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 Office of Management and Budget’s (OMB) fiscal year 2022 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 core areas.

These core areas align to requirements outlined in Executive Order 14028, *Improving the Nation’s Cybersecurity*, as well as recent OMB guidance on modernizing federal cybersecurity. The guidance notes that level 4 (*managed and measurable*) represents an effective level of security.