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

Executive Summary, 2021-IT-B-014, October 29, 2021

2021 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 several steps to strengthen its information security program. For instance, the Board has matured its software asset management processes and has developed a catalog of software installed on Board devices.

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. For example, within the *identify* function area, we noted opportunities to strengthen the Board's cybersecurity risk management processes. Specifically, we noted that key information, such as finding severity level and remediation start and end dates, was not being captured for the majority of weaknesses identified within the Board's system-level plans of action and milestones. Further, we found that the majority of the agency's documented system-level risk acceptances did not include an expiration date indicating when the Board's risk decision should be reassessed. We also identified the need for improvements in the implementation of the Board's software and license asset management processes for one of the agency's divisions. 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.

Finally, the Board has taken sufficient actions to close 8 of the 15 recommendations from our prior FISMA audit reports that remained open at the start of this audit. The closed recommendations relate to risk management, identity and access management, and information security continuous monitoring. We are leaving open 7 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 spring 2022 semiannual report to Congress and continue to monitor the Board's progress as part of future FISMA audits.

Recommendations

This report includes two new recommendations 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 recommendations and notes that actions are underway to strengthen the agency's information security program. We will continue to 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 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 fiscal year 2021 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.