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

Executive Summary, 2023-SR-B-010, June 26, 2023

Results of Scoping of the Evaluation of the Board and Reserve Banks' Cybersecurity Incident Response Process for Supervised Institutions

Findings

As part of our scoping efforts, we identified findings and recommendations that we believe the Board of Governors of the Federal Reserve System should implement to enhance the cybersecurity incident response process. We found that the Board can update guidance to clarify the mission and the governance structure of the cybersecurity incident response process. A clearly defined mission and governance structure for the cybersecurity incident response process should help guide the efforts of the parties involved and help enhance the effectiveness of the Board and Federal Reserve Banks' response to cybersecurity incidents.

We also found that the Board and Reserve Banks' responses to cybersecurity incidents have not consistently followed the process prescribed in guidance. In addition, multiple interviewees indicated that some stakeholders in the cybersecurity incident response process are unclear on their roles and responsibilities and that training would be beneficial. Clearly documenting the cybersecurity incident response process and the roles and responsibilities of key stakeholders, and providing training on these topics, will enhance the effectiveness of the Board and Reserve Banks' response when a cybersecurity incident occurs at a supervised institution.

We believe that these enhancements will improve the effectiveness of the cybersecurity incident response process and that the Board should prioritize addressing these items. We are communicating these items at the end of our scoping effort as these items may aid the Division of Supervision and Regulation's (S&R) assessment of refinements to the cybersecurity incident response process as part of its projects to enhance the process.

Recommendations

Our report contains recommendations designed to enhance the cybersecurity incident response process. In its response to our draft report, the Board concurs with our recommendations and outlines actions to address them. We will follow up to ensure that the recommendations are fully addressed.

Purpose

We initiated an evaluation in August 2022 to assess the Board and Reserve Banks' cybersecurity incident response process for supervised institutions. We are issuing this report to communicate our findings and recommendations based on the results of our scoping.

Background

Cybersecurity risks present significant and dynamic challenges to financial institutions. A significant cybersecurity incident at a Board-supervised financial institution could disrupt its operations and ultimately affect financial stability. *Cybersecurity incidents* occur through the use of computer networks and result in an actual or potentially adverse effect on the confidentiality, integrity, or availability of an institution's information systems or the information residing therein.

In response to the increasing frequency and sophistication of cybersecurity incidents at Board-supervised institutions and their service providers, S&R developed a playbook that seeks to establish procedures and protocols for effective, consistent, and replicable supervisory actions in response to cybersecurity incidents.