Executive Summary:

2015 Audit of the Board's Information Security Program

2015-IT-B-019 November 13, 2015

Purpose

To meet our annual Federal Information Security Modernization Act of 2014 (FISMA) reporting responsibilities, we reviewed the information security program and practices of the Board of Governors of the Federal Reserve System (Board). Our specific audit objectives, based on the legislation's requirements, were to evaluate (1) the Board's compliance with FISMA and related information security policies, procedures, standards, and guidance and (2) the effectiveness of security controls and techniques for a subset of the Board's information systems.

Background

FISMA requires federal agencies to develop, document, and implement an agency-wide information security program. FISMA also requires each Inspector General (IG) to conduct an annual independent evaluation of the agency's information security program and practices. The U.S. Department of Homeland Security (DHS) has issued guidance to IGs on FISMA reporting for 2015. The guidance directs IGs to evaluate the performance of agencies' information security programs across 10 areas. These areas are continuous monitoring, configuration management, identity and access management, incident response and reporting, risk management, security training, plan of action and milestones, remote access management, contingency planning, and contractor systems.

Findings

Overall, we found that the Board's Chief Information Officer has developed, documented, and implemented an information security program that is generally consistent with the requirements established by FISMA and the 10 areas outlined in DHS's FISMA reporting guidance for IGs. This year, we found that the Board has taken steps to mature the organization's information security continuous monitoring (ISCM) program through the development of metrics and monitoring frequencies. We also found that the Board has strengthened its risk management processes by automating the collection and review of plans of actions and milestones, and enhanced its contractor oversight processes to better ensure that third-party systems meet FISMA and Board requirements.

While we found the Board's information security program to be consistent with requirements outlined in DHS's FISMA reporting guidance for IGs, we identified further opportunities to strengthen the program in the areas of ISCM, configuration management, and identity and access management. Specifically, we found that the Board can mature its ISCM program through greater centralization and automation in the areas of people, processes, and technology; develop and implement a process to manage database-level vulnerabilities using automated tools for a key database technology used in the organization; and improve access controls for sensitive Board information maintained in the organization's enterprise-wide collaboration tool.

Recommendations

Our report includes four recommendations to improve the Board's information security program in the areas of ISCM, configuration management, and identity and access management. In her response to our report, the Director of the Division of Information Technology concurs with our recommendations and notes that actions are underway to address them. Further, based on corrective actions taken by the Board's Information Security Officer, we are closing the open recommendations from our prior years' FISMA reports related to contractor systems, ISCM, and plan of action and milestones.