Executive Summary:

2016 Audit of the Board's Information Security Program

2016-IT-B-013 November 10, 2016

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 the effectiveness of the Board's (1) security controls and techniques and (2) information security policies, procedures, and practices.

Background

FISMA requires each agency Inspector General (IG) to conduct an annual independent evaluation of the agency's information security program, practices, and controls for select systems. The U.S. Department of Homeland Security has issued guidance to the IGs on FISMA reporting for 2016. The guidance directs the IGs to evaluate the performance of their agencies' information security programs across eight domains that are grouped into five function areas: identify, protect, detect, respond, and recover.

Findings

Overall, we found that the Board continues to mature its information security program to ensure that it is consistent with FISMA requirements. For instance, the organization has implemented an enterprise-wide information security continuous monitoring lessons-learned process as well as strengthened its system-level vulnerability management practices. We also found that the Board's information security program contained policies and procedures that are generally consistent with the requirements for all eight information security domains listed by the U.S. Department of Homeland Security: risk management, contractor systems, configuration management, identity and access management, security and privacy training, information security continuous monitoring, incident response, and contingency planning. However, in the domain of risk management, we found that the Board can strengthen its insider threat activities by incorporating considerations for all types of sensitive information maintained by the organization into an organization-wide insider threat program. We also found that Board divisions were not consistently implementing the organization's risk management processes related to security controls assessment, security planning, and authorization.

In addition, we identified opportunities to strengthen controls in the areas of identity and access management, security and privacy training, and incident response to ensure that they are effective. Specifically, we identified opportunities for the Board to mature its information security program by (1) implementing a continuous monitoring approach for reviewing access to sensitive information maintained in the organization's enterprise-wide collaboration tool; (2) determining how best to implement multifactor authentication for all nonprivileged information system users; (3) conducting exercises to test the effectiveness of its security and privacy awareness training program; and (4) developing a plan to implement the Trusted Internet Connections Initiative and the governmentwide EINSTEIN program to better prevent, detect, and respond to information security incidents.

Finally, the Board has made progress in addressing our recommendations from last year's FISMA audit report. Our 2015 FISMA audit report included four recommendations to strengthen the Board's information security continuous monitoring, configuration management, and identity and access management. Based on the steps taken by the Board, we are closing three of our four outstanding recommendations.

Recommendations

Our report includes nine new recommendations to strengthen the Board's information security program in the areas of risk management, identity and access management, security and privacy training, and incident response. The Director of the Division of Information Technology concurs with our recommendations and stated that she has initiated actions to address them.