Executive Summary:
2013 Audit of the Board's Information Security Program

2013-IT-B-019 November 14, 2013

Purpose

To meet our annual Federal Information Security Management Act of 2002 (FISMA) reporting responsibilities, we reviewed the information security program and practices of the Board of Governors of the Federal Reserve System (Board).

Background

FISMA requires federal agencies to develop, document, and implement an agency-wide information security program. FISMA also requires each Inspector General to conduct an annual independent evaluation of its agency's information security program and practices.

Findings

Overall, we found that the Board's Chief Information Officer is maintaining a FISMA-compliant approach to the Board's information security program that is generally consistent with requirements established by the National Institute of Standards and Technology and the Office of Management and Budget.

The Board's Information Security Officer continues to issue policies and procedures that include attributes identified within the Department of Homeland Security (DHS) reporting metrics. In our response to the 11 DHS reporting metrics for 2013, we found that the Board has effective programs in place that are consistent with FISMA requirements and that include attributes identified by DHS for plan of action and milestones, remote access management, identity and access management, contingency planning, configuration management, and security capital planning. We also found that the Board has programs in place that include attributes identified within the DHS reporting metrics for incident response and reporting, security training, and contractor systems; however, our report identifies opportunities for improvement within those areas. Our report includes a recommendation related to tracking training for individuals with significant information security responsibilities and keeps open our 2012 recommendations related to incident reporting and contractor systems.

During the past year, the Information Security Officer has continued to make progress in implementing an enterprise information technology risk management framework and a continuous monitoring program; however, additional steps are needed to fully implement programs that are consistent with FISMA requirements. Our report includes a recommendation for continuous monitoring and keeps open our 2011 recommendation related to risk management.

Recommendations

We recommend that the Chief Information Officer continue to establish a continuous monitoring program by finalizing policies and procedures, establishing metrics, and defining the frequency of monitoring. We also recommend that the Chief Information Officer monitor specialized training taken by all individuals at the Board with significant responsibilities for information security to ensure that they have been adequately trained. In her response to our draft report, the Director of the Division of Information Technology, in her capacity as Chief Information Officer, agreed with the two recommendations and stated that she intends to take immediate action to address each recommendation.

Access the full report: http://www.federalreserve.gov/oig/files/FRB_Audit_Information_Security_FISMA_Nov2013.pdf
For more information, contact the OIG at 202-973-5000 or visit http://www.federalreserve.gov/oig.