Executive Summary:

2014 Audit of the Board's Information Security Program

2014-IT-B-019 **November 14, 2014**

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.

As part of an agency's annual FISMA reporting, the Office of Management and Budget (OMB) requests that both the Chief Information Officer (CIO) and the Inspector General perform analysis and report on certain information security program components. As discussed in OMB Memorandum 10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)*, the U.S. Department of Homeland Security (DHS) exercises primary responsibility within the executive branch for the operational aspects of federal agency cybersecurity with respect to FISMA.

Findings

Overall, we found that the Board's CIO 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 OMB. The Information Security Officer continues to issue policies and procedures to transition the Board's information security program to an integrated, organization-wide program for managing information security risks.

In analyzing the status of the Board's information security program in the 11 DHS reporting metrics for 2014, we found that the Board has effective programs in place that are consistent with FISMA requirements and that include attributes identified by DHS for risk management, security configuration, remote access, identity and access management, security training, incident response and reporting, and security capital planning. We also found that the Board has programs in place that include attributes identified within the DHS reporting metrics for continuous monitoring, contractor oversight, contingency planning, and plan of action and milestones; however, we identified opportunities for improvement within those areas. Our findings related to contingency planning are being reported under separate cover.

Recommendations

Our report includes one new recommendation for improving the tracking of division-level plans of action and milestones and keeps open our 2012 recommendation on contractor systems and our 2013 recommendation on continuous monitoring.

The Director of the Division of Information Technology stated that she agrees with the recommendation and that the division will take immediate action to address the recommendation, including continuing to manually collect quarterly plan of action and milestones reports from the offices and divisions until the automated plan of action and milestones tracking process is fully implemented.