Executive Summary:

Opportunities Exist to Improve the Operational Efficiency and Effectiveness of the Board's Information Security Life Cycle

2014-IT-B-021 December 18, 2014

Purpose

Our objectives for this audit were (1) to assess the processes the Board of Governors of the Federal Reserve System (Board) employs to meet Federal Information Security Management Act of 2002 (FISMA) requirements for security categorization, certification and testing, security plans, and accreditation of its information systems and (2) to review how the Board compiles its FISMA documents and review activities within its automated workflow support tool. In addition, we analyzed the Board's recently adopted risk management framework (RMF) document against National Institute of Standards and Technology (NIST) guidance.

Background

Information security life cycle refers to prescribed activities that must be performed for each Board information system throughout the various stages of the system's creation and existence. The Board has developed a FISMA-compliant approach to managing and evaluating a Board information system throughout its entire life cycle. Information security life cycle tasks begin early in the system development life cycle and shape the security capabilities of the information system. The Board manages its information security program through a collection of policies and procedures and supporting appendixes called the *Board Information Security Program*.

Findings

Overall, we found that the Chief Information Officer (CIO) maintains a FISMA-compliant information security program that is consistent with requirements for certification and accreditation established by NIST and OMB; however, we identified opportunities to improve the operational efficiency and effectiveness of the Board's management of its information security life cycle. First, we found that elements of the Board's information security life cycle were missing for some systems. Additionally, we found that the Information Security Officer developed a program to implement the requirements of NIST's RMF and issued the *Risk Management Program and Risk Assessment Standard* document in June 2014. The document, however, is not intended to include all of the recommended NIST requirements. Some of the processes are documented in the *Board Information Security Program* appendixes, but the appendixes have not been updated to reflect the new RMF process as well as new NIST guidance. Without up-to-date guidance, individuals responsible for managing Board systems may be unaware of their roles and responsibilities.

Recommendations

Our report contains three recommendations that are designed to improve the operational efficiency and effectiveness of the Board's information security life cycle process. We recommend that the Chief Information Officer (CIO) evaluate the automated workflow tool and determine any improvements needed to ensure it can meet documentation requirements of the Board's information security life cycle processes. We also recommend that the CIO ensure that system owners develop and input the security documentation for all Board-owned and -operated systems into the automated workflow tool. Finally, we recommend that the CIO perform a thorough reconciliation between the existing policy documents and the new *Risk Management Program and Risk Assessment Standard* to determine which processes remain relevant and update the applicable policy documents.

The Director of the Division of Information Technology stated that she agrees with the recommendations and that the division will take action to address the recommendations. We plan to follow up on the division's actions to ensure that the recommendations are fully addressed.