Executive Summary:

Security Control Review of the Board's Statistics and Reserves System

Purpose

The Federal Information Security Management Act of 2002 (FISMA), as amended by the Federal Information Security Modernization Act of 2014, requires the Office of Inspector General to evaluate the effectiveness of the information security controls and techniques for a subset of the Board of Governors of the Federal Reserve System's (Board) information systems, including those provided or managed by another agency, a contractor, or another organization. To meet this requirement, we reviewed the information system security controls for the Board's Statistics and Reserves System (STAR).

Our audit objective was to evaluate the adequacy of selected information security controls for protecting Board data in STAR from unauthorized access, modification, destruction, or disclosure, as well as the system's compliance with FISMA and the information security policies, procedures, standards, and guidelines of the Board.

Background

STAR was implemented in 1998 as a mainframe system supporting the statistics and reserves functions at the Board and the Federal Reserve Banks, and it is being modernized to a Web-based application. The system collects and edits over 75 periodic statistical reports that are received from financial institutions. In addition, the system manages financial institutions' reserve requirements and term deposits. STAR is listed on the Board's FISMA inventory as a moderate-risk system. The Board's Division of Monetary Affairs and Division of Information Technology have overall responsibility to ensure that the requirements of FISMA and the *Board Information Security Program* are met for STAR.

Findings

Overall, we found that the Division of Monetary Affairs and the Division of Information Technology have taken several steps to implement information security controls for STAR, in accordance with the requirements of FISMA and the *Board Information Security Program*. For example, we found that the divisions have implemented information system backup, incident reporting, and change management controls, in accordance with FISMA requirements. However, we found that improvements are needed in the Board's security governance of STAR to ensure that information security controls are adequately implemented, assessed, authorized, and monitored.

Our report includes six recommendations that focus on strengthening information security controls related to planning, security assessment and authorization, contingency planning, auditing, access control, risk assessment, and system and information integrity. In comments to our draft report, the Director of the Division of Information Technology and the Deputy Associate Director of the Division of Monetary Affairs concur with our recommendations and outline actions that have been or will be taken to address them.

We will follow up on the implementation of each recommendation in this report as part of our future audit activities related to the Board's continuing implementation of FISMA. Given the sensitivity of information security review work, our reports in this area are generally restricted. Such is the case for this audit report.