Executive Summary:

Security Control Review of the Board's Consolidated Supervision Comparative Analysis, Planning and Execution System

2015-IT-B-015 September 2, 2015

Purpose

The Federal Information Security Management Act of 2002, as amended by the Federal Information Security Modernization Act of 2014 (FISMA), requires the Office of Inspector General to evaluate the effectiveness of the information security controls and techniques for a subset of the agency's information systems, including those provided or managed by another agency, a contractor, or another organization. We evaluated the adequacy of selected security controls implemented by the Board of Governors of the Federal Reserve System (Board) to protect the Consolidated Supervision Comparative Analysis, Planning and Execution System (C-SCAPE) from unauthorized access, modification, destruction, or disclosure. We also evaluated C-SCAPE's compliance with FISMA and the information security policies, procedures, standards, and guidelines of the Board.

Background

C-SCAPE is a data input and reporting tool used by the Board's Division of Banking Supervision and Regulation to improve its oversight and supervision of large or systemically important financial institutions. C-SCAPE is intended to provide supervisory teams with tools and methods to plan and execute supervisory events, manage issues, and enhance decision making around the examination planning process.

Findings

Overall, we found that the Board has taken steps to secure the C-SCAPE application in accordance with FISMA and the Board's information security program. However, during vulnerability scanning of the databases supporting C-SCAPE, we found vulnerabilities that require the attention of the C-SCAPE application owner and the Board's Division of Information Technology.

Additionally, we noted one security-related issue: The C-SCAPE application audit logs do not record certain database activity on financial institution information. This issue was identified in the *2014 Security Assessment Report* completed by the Division of Information Technology's Compliance group. At the completion of our audit fieldwork, this issue had not been remediated.

Our report includes three recommendations to address C-SCAPE database vulnerabilities. We have also identified items for management's consideration that are already being addressed by management.

The Chief Information Officer and the Director of the Division of Banking Supervision and Regulation agreed with our recommendations. They have already begun taking actions on two recommendations and will address the third recommendation subject to the availability of emerging guidance from the Office of Management and Budget.

Given the sensitivity of information security review work, our reports in this area are generally restricted. Such is the case for this audit report.