



Executive Summary:

Security Control Review of a Third-party Commercial Data Exchange Service Used by the Board's Division of Banking Supervision and Regulation

2013-IT-B-010

August 6, 2013

Purpose

The Federal Information Security Management Act of 2002 (FISMA) 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's) information systems, including those provided or managed by another agency, a contractor, or another organization. As part of our work to fulfill this requirement, we reviewed the information system security controls for a third-party commercial data exchange service.

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

Background

The Division of Banking Supervision and Regulation (BS&R) uses the commercial data exchange service to securely exchange sensitive business information with financial institutions. The service is listed on the Board's FISMA inventory as a third-party application maintained by the Federal Reserve Bank of Philadelphia. BS&R is assigned overall responsibility for ensuring that the system meets FISMA requirements.

Findings

Overall, we found that the Board has taken steps to secure the third-party commercial data exchange service. However, we found that improvements are needed to ensure that the requirements of FISMA and the *Board Information Security Program* are met. Our report includes 11 recommendations to BS&R to strengthen security controls for the system.

In comments to our draft report, the Director of the Division of Banking Supervision and Regulation concurred with 10 recommendations and partially concurred with 1 recommendation. For the 10 recommendations with which the Director concurred, the actions he outlined that have been taken, are underway, and are planned address our recommendations. For the recommendation with which he partially concurred the Director outlined planned actions that are responsive to the intent of our recommendation. 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.