Office of Inspector General

Executive Summary

Independent Evaluation of the FDIC's Information Security Program—2009

Report No. AUD-10-001
November 2009

Why We Did The Audit

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies, including the FDIC, to have annual independent evaluations by agency Inspectors General of their information security program and practices and to report the results of the evaluation to the Office of Management and Budget (OMB). The FDIC Office of Inspector General (OIG) contracted with KPMG, LLP (KPMG) to perform an audit to fulfill the requirements for the 2009 independent evaluation. The objective of the audit was to determine the effectiveness of the FDIC's information security program and practices, including the FDIC's compliance with FISMA and related information security policies, procedures, standards, and guidelines.

Background

Key to achieving the FDIC's mission of maintaining stability and public confidence in the nation's financial system is safeguarding sensitive information. Ensuring the confidentiality, integrity, and availability of this information in an environment of increasingly sophisticated security threats requires a strong, corporate-wide information security program.

The National Institute of Standards and Technology (NIST) has developed information security standards and guidelines, including recommended security controls, for Federal information systems and organizations. NIST has organized recommended security controls into families that define the security control structure.

Audit Results

The FDIC has established a corporate-wide information security program, including policies and procedures, addressing the principal provisions of FISMA and the standards and guidelines of the NIST. The FDIC had also implemented a number of important security control improvements following KPMG's 2008 evaluation, such as encrypting mainframe and server backup tapes, developing a multi-year strategy for generating and reviewing audit logs for the FDIC's portfolio of information systems, and restricting access to security logs from network devices. Additional control improvements were underway at the close of the audit.

The above accomplishments were positive. However, KPMG identified a number of security program control families warranting management attention. Most notably, KPMG identified access control deficiencies within the FDIC's internal network similar to those identified in the 2008 FISMA evaluation that presented a high risk of unauthorized disclosure of sensitive information or compromise of information technology resources. While the FDIC took prompt action to address the specific access control vulnerabilities identified during the audit, priority management attention in this area continues to be warranted.

The report identifies nine steps that the Corporation can take to strengthen its information security controls. These steps address such areas as: Enterprise Architecture; Risk Assessment; Planning; Certification, Accreditation, and Security Assessments; Physical and Environmental Protection; Configuration Management; Identification and Authentication; Access Control; and Audit and

Accountability. In many cases, the FDIC was already working to improve security controls in these areas during KPMG's audit.

We will issue our responses to specific questions raised by OMB in its August 20, 2009 memorandum, FY 2009 *Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* through the OMB automated collection tool. Our responses to the OMB questions, together with the independent security evaluation report, satisfy our 2009 FISMA reporting requirements.

Because this report addresses sensitive issues associated with information security, we do not intend to make public release of the specific contents of the report.