Office of Inspector General

Executive Summary

Independent Evaluation of the FDIC's Information Security Program—2011

Report No. AUD-12-002
October 2011

Why We Did The Audit

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies, including the FDIC, to perform annual independent evaluations of their information security programs and practices and to report the evaluation results to the Office of Management and Budget (OMB). FISMA states that the independent evaluations are to be performed by the agency Inspector General (IG), or an independent external auditor as determined by the IG. The objective of this performance audit was to evaluate 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 the sensitive information that the Corporation collects and manages. 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.

FISMA directs the National Institute of Standards and Technology (NIST) to develop risk-based standards and guidelines to assist agencies in defining security requirements for their information systems. In addition, OMB issues information security policies and guidelines, including annual instructions to the heads of federal executive departments and agencies for meeting their reporting requirements under FISMA. The Department of Homeland Security (DHS) exercises primary responsibility within the Executive Branch for the operational aspects of federal agency cybersecurity with respect to the federal information systems that fall within the scope of FISMA. DHS's responsibilities include overseeing agency compliance with FISMA and developing analyses for OMB to assist in the development of OMB's annual FISMA report to the Congress. In this regard, DHS provided agency IGs with a set of security-related questions to address their FISMA reporting responsibilities in a June 1, 2011 document entitled, *FY 2011 Inspector General Federal Information Security Management Act Reporting*.

We evaluated the effectiveness of the FDIC's information security program and practices by designing audit procedures to assess consistency between the FDIC's security controls and FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines in the areas covered by the DHS questions. In addition, we engaged KPMG LLP to provide audit assistance in certain security control areas. We are required to be submit our responses to the DHS questions through OMB's FISMA reporting platform—CyberScope—by November 15, 2011.

Audit Results

We concluded that, except as noted below, the FDIC had established and maintained information security program controls that were generally consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines for the security control areas that we evaluated. Of particular note, the FDIC had established security policies and procedures in almost all of the security control areas evaluated. In addition, the FDIC continued its prior-year efforts to implement current and emerging security standards and guidelines published by NIST, such as updating its security plan template to reflect new NIST guidelines. The FDIC had also implemented various security control

improvements following our prior-year security evaluation. Most notably, the FDIC made meaningful progress in developing an agency-wide continuous monitoring program to evaluate the security of its information systems and hired additional information security managers to support and administer security over its general support systems and major applications.

Notwithstanding the above achievements, priority management attention continues to be warranted in some security control areas, particularly continuous monitoring management. Specifically, significant work remains before the FDIC's agency-wide continuous monitoring program is fully implemented. In addition, risk in the area of contractor systems remains elevated as a result of the FDIC's continued heavy reliance on contractors to support its bank resolution and receivership activities. While the FDIC has developed a formal methodology for assessing risks associated with its contractor systems, work remains to fully apply this methodology to all of the FDIC's outsourced information service providers. Maintaining vigilance in these and other areas of the FDIC information security program will continue to be important given other corporate priorities associated with the current banking environment.

Recommendations and Management Comments

The report includes seven recommendations intended to improve the effectiveness of the FDIC's information security program controls in the areas of plans of action and milestones, remote access management, identity and access management, and contractor systems. In many cases, the FDIC was already working to strengthen security controls in these areas during our audit. Our report does not include recommendations in the area of continuous monitoring management as the FDIC was working to fully implement a multi-year effort to address a recommendation in our prior-year security evaluation report required by FISMA.

On October 27, 2011, the FDIC's Chief Information Officer (CIO), who also serves as Director, Division of Information Technology, provided a written response to a draft of this report. In the response, the CIO concurred with all seven of the report's recommendations and described planned corrective actions that were responsive.

The report contains sensitive information concerning the FDIC's information security program. Accordingly, we do not intend to release the report publicly.