Office of Inspector General

Executive Summary

Independent Evaluation of the FDIC's Information Security Program—2012

Report No. AUD-13-003
November 2012

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, including personally identifiable information, that the FDIC collects and manages in its role as federal deposit insurer and regulator of state non-member financial institutions. As an employer, an acquirer of services, and a receiver for failed institutions, the FDIC also obtains considerable amounts of sensitive information from its employees, contractors, and failed institutions. Further, the FDIC has begun collecting sensitive information, such as resolution plans for systemically important financial institutions, pursuant to its responsibilities under the Dodd-Frank Wall Street Reform and Consumer Protection Act. Implementing proper controls over this information is critical to mitigating the risk of a negative financial impact upon insured institutions or an unauthorized disclosure that could lead to identity theft, consumer fraud, and potential legal liability or public embarrassment for the Corporation.

FISMA requires federal agencies, including the FDIC, to develop, document, and implement agency-wide information security programs to provide security for their information and information systems and to support the operations and assets of the agencies, including information and information systems that are provided or managed by another agency, contractor, or other source. 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 for federal information resources pursuant to various statutory authorities. In this regard, OMB issued Memorandum M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated October 2, 2012. This memorandum provides the heads of executive departments and agencies with instructions for meeting their reporting requirements under FISMA and for reporting on their privacy management programs.

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 formulating analyses for OMB's use in the development of its annual FISMA report to the Congress. DHS provided agency IGs with a set of security-related questions to address their FISMA reporting responsibilities in a March 6, 2012 document entitled, *FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics*.

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. We are required to submit our responses to the DHS questions through OMB's FISMA reporting platform—CyberScope—by November 15, 2012.

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. The FDIC also continued to make meaningful progress on a multi-year initiative to improve its agency-wide Continuous Monitoring controls designed to facilitate near real-time risk management and promote organizational situational awareness with regard to the state of security of the FDIC's information systems.

Notwithstanding the above achievements, management attention is warranted in several security control areas, particularly Plan of Action and Milestones (POA&Ms), Contractor Systems, and Risk Management. Specifically, planned actions to address a large number of high- and moderate-risk security vulnerabilities were significantly past their scheduled completion dates on POA&Ms, limiting the FDIC's assurance that sensitive information and information technology (IT) resources are adequately protected. In addition, risk in the area of Contractor Systems remains elevated due to the FDIC's continued heavy reliance on contractors to support bank resolution and receivership activities. While the FDIC has developed a risk-based strategy and formal methodology for assessing risks associated with Contractor Systems, significant work remains to apply the methodology to all of the FDIC's outsourced information service providers. With respect to Risk Management, our report describes an approach that the FDIC can take to help ensure that business-led application development efforts are incorporated into the FDIC's risk management framework and IT governance processes.

The FDIC's business divisions and offices play a critical role in the successful implementation of the FDIC's information security program, including those areas where we found that management attention was warranted. In this regard, the Chief Information Officer (CIO) will need to coordinate with other senior FDIC management officials to ensure that program-related priorities are balanced with the need to address the Corporation's information security requirements.

Recommendations and Corporation Comments

Our report contains 14 recommendations to improve the effectiveness of the FDIC's information security program controls. In many cases, the FDIC was already working to strengthen security controls in these areas during our audit. We identified certain other potential control enhancements that we did not consider significant within the context of the audit's objective. We communicated those matters separately to appropriate FDIC management officials.

On November 2, 2011, the FDIC's CIO, who also serves as Director, Division of Information Technology, and the Director, Division of Administration, provided a written response to a draft of this report. In the response, FDIC management concurred with all 14 of the report's recommendations and described planned corrective actions that were responsive.

Because this report contains sensitive information, we do not intend to make the report available to the public in its entirety. We will, however, post this Executive Summary on our public Web site.