Office of Inspector General

Executive Summary

Independent Evaluation of the FDIC's Information Security Program—2014

Report No. AUD-15-001
November 2014

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 controls and practices, including the FDIC's compliance with FISMA and related information security policies, procedures, standards, and guidelines. We evaluated the effectiveness of security controls by performing audit procedures to assess consistency between the FDIC's security controls and FISMA requirements, OMB policy and guidelines, and National Institute of Standards and Technology (NIST) standards and guidelines. The scope of the audit covered the 11 security control areas outlined in the Department of Homeland Security's (DHS) December 2, 2013, document entitled, *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*. Our work included an analysis of selected controls for three of the FDIC's general support systems and a review of the Corporation's oversight of an outsourced information service provider that supports the FDIC's marketing of failing financial institutions.

Background

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 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. Further, DHS exercises primary responsibility within the Executive Branch for the operational aspects of federal agency cyber security 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.

Audit Results

We concluded that, except as described below, the FDIC had established and maintained many information security program controls and practices that were generally consistent with FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines. The FDIC had also taken action subsequent to our prior-year security evaluation to strengthen controls in a number of the areas that we evaluated, including:

- *Incident Response and Reporting*—by strengthening procedures and guidance for addressing computer security incidents and communicating those incidents to senior FDIC management;

- *Risk Management*—by issuing a formal policy that subjects all application development efforts—including those managed by the FDIC's business divisions or offices—to appropriate information security risk management and information technology (IT) governance; and

- *Outsourced Information Systems and Services*—by establishing more meaningful metrics pertaining to oversight activities, making progress in completing those oversight activities, and beginning to require stronger security and privacy clauses for newly-awarded service agreements administered by the Legal Division.

In addition, the FDIC had implemented 17 of 19 recommendations from our 2012 and 2013 security evaluation reports that were unaddressed as of November 21, 2013, and was working to address the remaining two recommendations at the close of our audit.

Notwithstanding these accomplishments, we found that management attention was warranted in the security control areas of:

- *Risk Management*. The FDIC was revising its IT security risk management program policy to align with OMB policy and NIST guidelines. The FDIC can further its efforts in this area by adopting (i.e., tailoring, documenting, and approving) new or modified security controls, as appropriate, consistent with NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, dated April 2013.

- *Continuous Monitoring*. The FDIC was performing a number of continuous monitoring activities and had developed an assessment methodology for monitoring at the information systems level. However, the FDIC had not developed a written, corporate-wide information security continuous monitoring strategy as required by OMB policy.

- *Configuration Management*. The FDIC was working on a multi-year effort to develop baseline configurations for its information systems and strengthen its vulnerability and patch management program. As part of that effort, the Corporation needs to develop written procedures to ensure that newly-released operating system patches are tested in a consistent manner and that test results are adequately documented.

- *Plan of Action and Milestones (POA&M)*. The FDIC had several initiatives underway to improve its POA&M process. The FDIC can further these efforts by (a) reviewing and enhancing (where appropriate) existing controls designed to ensure that security vulnerabilities are recorded on POA&Ms in a timely manner and (b) conducting an internal assessment of the effectiveness of the POA&M process after a reasonable period of time is allowed for the implementation of planned and ongoing improvement initiatives.

- *Contingency Planning*. The FDIC made meaningful progress in addressing our prior year recommendations in this area. At the time of our audit, the FDIC was working to complete ongoing analysis to confirm the appropriateness of established recovery time objectives for systems supporting mission-essential functions.

Addressing the issues described above will better align the FDIC's security program controls with FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines. It will also facilitate the identification, evaluation, and mitigation of risk to the FDIC's information and information systems.

Recommendations and Corporation Comments

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

On October 30, 2014, the FDIC's Acting Chief Information Officer (CIO) provided a written response to a draft of this report. In the response, the Acting CIO concurred with all five of the report's recommendations and described ongoing and 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.