Office of Inspector General

Executive Summary

Independent Evaluation of the FDIC's Information Security Program—2013

Report No. AUD-14-002
November 2013

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 nonmember 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. Implementing proper controls over this information in an environment of increasingly sophisticated security risks and global connectivity underscores the importance of a strong, enterprise-wide information security program.

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. Further, the Department of Homeland Security (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.

To address our objective, we performed audit procedures to evaluate the 11 security control areas outlined in DHS' November 30, 2012 document entitled, *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*. We evaluated the effectiveness of security controls in these areas 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. Our work included testing of selected servers and desktops and a review of the FDIC's oversight of an outsourced information service provided by Innovative Discovery.

Audit Results

We concluded that 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 applicable NIST standards and guidelines. Notably, the FDIC had established security policies and procedures in almost all of the security control areas we evaluated. The FDIC was also working to develop a formal concept-of-operations document that describes a corporate-wide approach to information security continuous monitoring.

To address current and emerging risks in the information technology (IT) and information security environments, the FDIC made significant changes to its security governance structure during 2013. Such changes included the realignment of the roles and responsibilities of the Chief Information Officer (CIO), Chief Information Security Officer, and Information Security and Privacy Staff. The FDIC also established an IT/Cyber Security Oversight Group to provide a senior-level forum for addressing cyber security threats and developments impacting both the FDIC and the banking industry. Such changes are positive and better position the FDIC to address information security risks from a corporate perspective. We plan to more fully assess the implementation of these security governance changes as part of our future audit and evaluation work.

Notwithstanding these accomplishments, we determined that continued management attention and control improvements are needed to more effectively identify, evaluate, and mitigate risk to the FDIC's information systems and data, particularly in the areas of *Incident Response and Reporting*, *Risk Management*, *Configuration Management*, *Outsourced Information Systems and Services*, and *Contingency Planning*. Specifically, the FDIC needed to strengthen its incident response policies and procedures to address sophisticated, cyber-based security incidents and update its corporate information security risk management policy to reflect changes in its risk management processes and governance. The FDIC can also take additional steps to help ensure that certain servers and workstations are patched to protect against known vulnerabilities. In addition, greater emphasis needs to be placed on assessing risks associated with the FDIC's outsourced information systems and services where limited progress has been made in the last year. Finally, further analysis is warranted to ensure that information systems supporting mission essential functions can be recovered within the timeframes needed to support those functions.

Recommendations and Corporation Comments

Our report contains 15 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 November 19, 2013, the Acting CIO and the Director, Division of Administration, provided a written response to a draft of this report. In the response, FDIC management concurred with all 15 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.

Reliability of Previously-Issued FISMA Audit Reports

In a memorandum entitled, *Planned Actions to Address New Information Associated with Previously Issued Audit Reports on the FDIC's Information Security Program*, dated May 30, 2013, the IG notified the FDIC Chairman that the OIG had become aware of new information related to the FDIC's information security program that could affect the reliability of certain findings and conclusions in our prior audit reports, entitled *Independent Evaluation of the FDIC's Information Security Program—2011* (Report No. AUD-12-002, dated October 31, 2011) and *Independent Evaluation of the FDIC's Information Security Program—2012* (Report No. AUD-13-003, dated November 5, 2012). These reports were not made available to the public due to the sensitive nature of the information they contained. Only the reports' Executive Summaries, which did not contain sensitive information, were posted on the OIG's public Web site.

Consistent with *Government Auditing Standards*, we provided notice on our public Web site and to users of the referenced FISMA reports that the associated findings and conclusions may not be reliable. As part of this year's audit, we performed expanded audit procedures to assess the impact of the new information on the findings and conclusions in the earlier reports. Based on those procedures, we determined that the findings and conclusions related to *Incident Response and Reporting* and *Risk Management* in both reports were not reliable, but that the reports' other findings and conclusions were reliable and the associated recommendations were valid. The results of our expanded audit procedures are described in our current year FISMA report. We plan to post a new notice on our public Web site that accompanies the Executive Summaries and clarifies the findings and conclusions therein for the two prior-year reports.