Office of Inspector General

Office of Audits and Evaluations
Report No. AUD-16-001

Audit of the FDIC's Information Security Program—2015

This report contains sensitive information and is for official use only. Other than the Executive Summary, the contents of the report are not releasable without the approval of the Office of Inspector General.

October 2015

Office of Inspector General

Executive Summary

Audit of the FDIC's Information Security Program—2015

Report No. AUD-16-001
October 2015

Why We Did The Audit

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including the FDIC, to perform annual independent evaluations of their information security programs and practices and to report the results to the Office of Management and Budget (OMB). This Act replaced provisions of the Federal Information Security Management Act of 2002. 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 FDIC Office of Inspector General (OIG) engaged the professional services firm of Cotton & Company LLP (C&C) to conduct a performance audit to satisfy this FISMA requirement.

The objective of this performance audit was to evaluate the effectiveness of the FDIC's information security program and practices. To address the objective, C&C performed audit procedures to evaluate the 10 security control areas outlined in the Department of Homeland Security's (DHS) June 19, 2015, document entitled, *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*. C&C's work included an analysis of selected security controls related to two of the FDIC's general support systems and two major applications, as well as a review of the Corporation's risk management activities related to an outsourced information service provider that facilitated employee recruitment efforts.

Background

FISMA requires federal agencies 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, under FISMA, and in consultation with OMB, DHS administers the implementation of agency information security policies and practices for information systems. DHS's responsibilities include developing operational directives regarding such matters as reporting security incidents and providing operational and technical assistance to agencies in implementing information security-related guidance.

Audit Results

Overall, C&C concluded that, except as described below, the FDIC's information security program and practices were generally effective. As part of the firm's work, C&C noted several important improvements in the FDIC's information security program over the last year. Specifically, the FDIC:

- enhanced its patch and vulnerability management program through the creation of a Patch and Vulnerability Management Group (PVG) and related subgroups that meet regularly to evaluate technical vulnerabilities in the FDIC's Information Technology (IT) environment and work to implement solutions;

- improved its process for managing known security weaknesses through Plans of Actions and Milestones (POA&Ms) as demonstrated by a reduction in the number of open high-risk POA&Ms from 49 in September 2014 to 26 in August 2015;

- expanded its security metrics reporting, particularly to senior management, which has resulted in increased awareness of information security risks and enabled management to take more proactive measures to improve the FDIC's overall information security posture; and

- revised its corporate information security risk management program policy to better align with NIST guidance.

In addition, the FDIC implemented five of seven previously unaddressed recommendations from our 2013 and 2014 security evaluation reports required by FISMA, and was working to address the remaining two recommendations at the close of the audit.

Notwithstanding these accomplishments, C&C identified aspects of the FDIC's information security program warranting management attention. Of particular note, the duties and role of the FDIC's Information Security Managers (ISM) in addressing information security requirements and risks within the FDIC's business divisions and offices have evolved since the ISM program was established. However, the FDIC had not recently completed a comprehensive assessment to determine whether the skills, training, oversight, and resource allocations pertaining to the ISMs enable them to effectively carry out their increased responsibilities and address security risks within their divisions and offices. In addition, the FDIC had not always ensured the timely completion of outsourced information service provider assessments or the timely review of user access to FDIC information systems. Further, the FDIC had not identified access control weaknesses for an outsourced information service provider that C&C found during its audit.

The FDIC was continuing its work on a multi-year initiative to develop secure baseline configurations for its information systems. Baseline configurations that are documented, implemented, and monitored are a critical control for ensuring that the FDIC's information systems are adequately protected. The FDIC was also working to implement multifactor authentication for nonprivileged network users and, separately, to perform system event logging and monitoring for certain databases. Continued management attention on each of these initiatives is warranted to ensure their success. C&C identified additional findings in the security control areas of risk management and configuration management that are described in the firm's report.

Finally, C&C noted that the FDIC depended heavily upon its infrastructure services contract (ISC) to support IT operations and implement security controls. C&C noted certain risks associated with the ISC, that, if not properly managed, could negatively impact the FDIC's IT operations, including its security operations. FDIC officials informed C&C that they were aware of these risks and were taking steps to mitigate them.

Recommendations and Corporation Comments

The report contains five recommendations addressed to the Acting Chief Information Officer (CIO) and one recommendation addressed to the Director, Division of Administration (DOA), that are intended to

improve the effectiveness of the FDIC's information security program controls and practices. The Acting CIO and Director, DOA, provided a joint written response, dated October 23, 2015, to a draft of C&C's report. In the response, FDIC management concurred with all six of the report's recommendations and described planned and completed actions that were responsive to the recommendations.

C&C identified certain other matters during the audit that the firm did not consider significant in the context of the audit objective. The OIG plans to communicate these matters separately to appropriate FDIC management officials.

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