Office of Inspector General

Executive Summary

Audit of the FDIC's Information Security Program—2016

Report No. AUD-17-001
November 2016

Why We Did The Audit

The Federal Information Security Modernization Act of 2014 (FISMA), which replaced provisions of the Federal Information Security Management Act of 2002, 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). The statute states that the independent evaluations are to be performed by the agency Inspector General, or an independent external auditor as determined by the Inspector General. Accordingly, the FDIC Office of Inspector General (OIG) engaged the professional services firm of Cotton & Company LLP (C&C) to conduct this performance audit.

The objective of the audit was to evaluate the effectiveness of the FDIC's information security program and practices. The audit included a review of selected security controls related to four general support systems and the FDIC's risk management activities related to an outsourced information service provider supporting asset servicing functions. As part of its work, C&C performed audit procedures to develop responses to security-related questions contained in the Department of Homeland Security's (DHS) September 26, 2016 document, entitled *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*. We are transmitting C&C's responses to these questions through OMB's automated reporting tool – CyberScope. C&C's responses, together with this performance audit report, satisfy our 2016 reporting requirements under FISMA.

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

C&C found that the FDIC had established a number of information security program controls and practices that were generally consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines. For example, the FDIC had established policies in most of the security control areas that C&C reviewed; engaged an outside firm to test internal network security controls; and provided security awareness training to network users. The FDIC had also taken steps to strengthen its security program controls following the 2015 FISMA audit. Among other things, the FDIC:

- restricted (with limited exceptions) the ability of network users to copy information to removable media to reduce the risk of unauthorized exfiltration of sensitive information.

- identified and reported its high value assets (HVA) to DHS. As a next step, the FDIC will need to (1) review these HVAs and their associated business processes to determine how sensitive information related to HVAs moves throughout the FDIC's network, systems, and facilities, including where it is stored, and (2) determine whether additional security controls are warranted to better protect this information.

- updated its security control framework to address changes introduced by NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, dated April 2013.

Notwithstanding these actions, C&C's report describes security control weaknesses that impaired the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at elevated risk. C&C reported on a total of 17 findings, of which 6 were identified during the current year FISMA audit and the remaining 11 were identified in prior reports issued by the OIG or the Government Accountability Office (GAO). Findings from prior reports consist of control weaknesses that the FDIC was working to address, but had not yet fully remediated, and, therefore, continue to pose risk to the FDIC. These findings are annotated to reflect the year in which they were initially reported. In some cases, the previously-reported weaknesses are long-standing issues. The most notable weaknesses reported by C&C pertain to:

- **Strategic Planning.** Although the FDIC had an information security strategic plan, it expired in 2015 and does not fully reflect OMB's cybersecurity priorities or the FDIC's information technology (IT) strategies. The FDIC would significantly benefit from the development of a new, comprehensive information security strategic plan that links ongoing and planned IT initiatives to longer-term security and business goals and priorities.

- **Vulnerability Scanning.** The FDIC was not performing security vulnerability scanning for more than 900 (or one-third) of the production servers within one of the general support systems that C&C reviewed. This control weakness presented a significant security risk to the FDIC as it limited the FDIC's assurance that network vulnerabilities that could lead to unauthorized access or other malicious activity would be detected and addressed in a timely manner.

- **The Information Security Management Program (ISM Program) (2015).** Prior to the close of the audit, the FDIC completed an assessment of its ISM Program, which is designed to address information security requirements and risks within the FDIC's business divisions and offices. The assessment identified gaps in such areas as available resources, training, and performance measurement. The FDIC plans to complete all actions to address these gaps by 2018.

- **Configuration Management (2014).** The FDIC continued to work on a multi-year initiative to develop baseline configurations to help secure its information systems. However, more work remains to fully establish and implement baseline configurations for all of the FDIC's information systems.

- **Technology Obsolescence (2015).** The FDIC made meaningful progress in replacing outdated server technology within one of the general support systems that C&C reviewed. However,

elevated security and operational risk remains as outdated and unsupported server technology continues to be used to support IT services, including a mission critical service, for this system.

- **Third-Party Software Patching (2015).** A June 2016 FDIC vulnerability assessment report indicated that high severity vulnerabilities for two third-party software products existed on over 40 percent of the FDIC's 2,819 network production servers covered by the report. These vulnerabilities needed to be investigated and addressed.

- **Multi-factor Authentication (2013).** The FDIC was working to issue Personal Identity Verification Cards to all eligible employees and contractor personnel and planned to begin requiring the use of the cards as its multi-factor authentication solution to reduce the risk of unauthorized network access by the end of 2016.

- **Contingency Planning (2013).** The FDIC has been working on a multi-year project to assess its business functions and recovery capabilities and identify gaps that could impair the Corporation's ability to maintain its mission essential functions during a disruption. Priority management attention is needed to ensure that this assessment is brought to completion as soon as practical and that identified gaps are addressed.

- **Service Provider Assessments (2011).** The FDIC made meaningful progress towards completing timely assessments of its outsourced service providers following C&C's prior year audit. However, continued management attention is warranted in this area to ensure outstanding assessments are completed timely.

At the close of the audit, the FDIC was working to strengthen the effectiveness of its information security program controls in a number of other areas. For example, the FDIC was working to:

- improve its incident response capabilities by developing an overarching incident response program guide, updating incident response policies and procedures, hiring an incident response coordinator, and better documenting incident investigative activities;

- more effectively protect its sensitive information by improving the effectiveness of its Data Loss Prevention tool and adopting Digital Rights Management software;

- complete an end-to-end assessment of its information security and privacy programs;

- hire a permanent Chief Information Security Officer (CISO); and

- begin addressing action items identified during a CyberStat Review with OMB and DHS officials aimed at improving the FDIC's cybersecurity posture and accelerating progress towards addressing key Administration priorities.

C&C's report also discusses (1) a risk related to the FDIC's infrastructure services contract and (2) an observation on recent turnover in the CISO position and whether the CISO's authorities enable the CISO

to effectively address the responsibilities defined in FISMA. In C&C's view, these matters have security implications and warrant management's continued consideration.

Recommendations and Corporation Comments

C&C's report contains six new recommendations addressed to the CIO that are intended to improve the effectiveness of the FDIC's information security program and practices. The CIO provided a written response, dated October 27, 2016, to a draft of C&C's report. In the response, the CIO concurred with all six of the report's recommendations and described planned and completed actions to address each recommendation. At our request, the CIO subsequently clarified the actions described in the response for two of the six recommendations. We determined that management's planned and completed actions were responsive to all of the recommendations. With respect to the report's observation on the responsibilities, authorities, and recent turnover in the CISO position, the response indicated that management would consider the matter and document whether any changes to the CISO role are warranted by April 15, 2017.

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 those 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.