# Office of Inspector General

Office of Information Technology Audits and Cyber
Report No. AUD-18-001

## Audit of the FDIC's Information Security Program—2017

**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 2017

Office of Inspector General

**Executive Summary**

# Audit of the FDIC's Information Security Program—2017

Report No. AUD-18-001
October 2017

## 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). 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 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 three general support systems, one business application, and the FDIC's risk management activities pertaining to four outsourced information service providers. As part of its work, C&C developed responses to security-related questions contained in the Department of Homeland Security's (DHS) document, entitled *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics V 1.0*, dated April 17, 2017 (the IG FISMA 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 2017 reporting responsibilities under FISMA.

## Background

FISMA requires federal agencies to develop, document, and implement 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.

## 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. The FDIC had also taken, or was working to take, steps to strengthen its security program controls following the 2016 FISMA audit. Among other things, the FDIC:

- Developed and published an Information Technology (IT) Strategic Plan that includes goals for strengthening information security and privacy.

- Created a new Office of the Chief Information Security Officer to better position the FDIC to address information security and privacy issues.

- Issued Personal Identity Verification card credentials to its employees and contractor personnel and began requiring use of the cards to access the Corporate network via desktop and laptop computers.

- Updated a number of its information security and privacy policy directives to align with government-wide security policy and guidance.

Notwithstanding these actions, C&C's report describes security control weaknesses that limited 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 risk. C&C reported a total of 19 findings, of which 14 were identified during the current year FISMA audit and the other 5 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, continued to pose risk to the FDIC. The most notable weaknesses reported by C&C are described below.

**Contingency Planning.** The FDIC's IT restoration capabilities are limited, and the agency has not taken timely action to address known limitations with respect to its ability to maintain or restore critical IT systems and applications during a disaster. Therefore, the FDIC cannot be sure that it can maintain or restore its mission essential functions during an emergency within applicable timeframes. The FDIC developed a plan to address these contingency planning issues at the close of our audit. The FDIC should also implement appropriate governance over its efforts to strengthen the resiliency and availability of its IT systems and applications.

**Information Security Risk Management.** The FDIC established the Information Security Risk Advisory Council (the Council) in 2015. However, the Council did not fulfill several of its key responsibilities as defined in FDIC policy. Most notably, the Council did not develop information security risk management standards and guidelines, a security risk tolerance level, or a Corporate risk profile. Such standards and guidelines provide a systematic and repeatable methodology for divisions and offices to discuss information security risks and manage and prioritize those risks. Further, without established risk tolerance levels and a risk profile, decisions are made without the context of the acceptable level of risk that the FDIC is willing to accept.

**Enterprise Security Architecture.** The FDIC had not established an enterprise security architecture that (i) describes the FDIC's current and desired state of security and (ii) defines a plan for transitioning between the two. The lack of an enterprise security architecture increased the risk that the FDIC's information systems would be developed with inconsistent security controls that are costly to maintain.

**Technology Obsolescence.** The FDIC was using certain software in its server operating environment that was at the end of its useful life and for which the vendor was not providing support to the FDIC. When the vendor does not provide support for software components, adversaries can exploit new weaknesses. This placed portions of the FDIC's IT infrastructure at increased risk of malicious attacks and exploits.

**Assessments of Outsourced Information Service Providers.** The FDIC made progress towards completing timely security assessments of its outsourced service providers following the 2016 FISMA

audit. However, more work remains. Without timely assessments of outsourced service providers, the confidentiality, integrity, and availability of the FDIC's information is at risk.

**Information Security Strategic Plan.** The FDIC had drafted, but not yet finalized, an information security strategic plan. Such a plan is needed to help ensure that the FDIC's ongoing and planned IT initiatives are clearly linked to long-term security and business goals and priorities and that resources are directed toward priority areas.

**Patch Management.** C&C noted instances in which patches addressing high-risk vulnerabilities were not installed on servers, desktop computers, and laptop computers within the timeframes established by FDIC policy. Unapplied patches expose the FDIC to increased risk of system outages and unauthorized or malicious activity.

**Credentialed Scanning.** C&C noted instances in which network IT devices were not subject to a "credentialed" scan—a thorough type of scan that involves logging into the IT device to inspect for vulnerabilities. The FDIC needed to enhance its processes to ensure that issues associated with conducting credentialed scanning of network IT devices are resolved in a timely manner. This weakness limited the FDIC's assurance that network vulnerabilities would be detected and addressed in a timely manner.

**Security Information and Event Management (SIEM) Tool.** The FDIC had not developed a process to ensure that all servers on the FDIC's network route log data to the FDIC's SIEM tool. If all servers do not route log data to the SIEM tool, the data will not be analyzed, presenting a risk that security threats will not be detected.

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:

- strengthen its incident response capabilities by updating its breach response plan to align with OMB guidance and improving the documentation of incident investigation activities;
- improve its information security and data management practices by developing a corporate-wide data classification program; and
- help protect its IT systems and data from hackers and malicious insiders by segmenting its network.

**IG FISMA Reporting Metrics**

The IG FISMA Reporting Metrics are structured to align with the five function areas in NIST's *Framework for Improving Critical Infrastructure Cybersecurity*: Identify, Protect, Detect, Respond, and Recover. The IG FISMA Reporting Metrics require IGs to assign a maturity level rating for all five function areas, as well as an overall rating, using a scale of 1 – 5, where 5 is the highest rating. In general, lower level maturity ratings focus on defining policies, procedures, and strategies while higher level ratings focus on measuring and optimizing performance. We assigned a maturity level rating of 2, "Defined," for each of the five function areas and for the FDIC's overall information security program. A

rating of 2 indicates that the FDIC's policies, procedures, and strategies were generally formalized and documented but not consistently implemented. It should be noted that changes have been made to the reporting metrics used by IGs in recent years. These changes, together with differences in the scope of audit work performed each year, make it difficult to compare this year's maturity level ratings to prior year ratings.

## Recommendations and Corporation Comments

C&C's report contains 18 recommendations addressed to the FDIC's Chief Information Officer (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 23, 2017, to a draft of C&C's report. In the response, the CIO concurred with all 18 of the report's recommendations and described planned corrective actions to address 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 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.