Office of Inspector General

Executive Summary

The FDIC's Information Security Program–2018

The Federal Information Security Modernization Act of 2014 (FISMA), Public Law No. 113-283, requires Federal agencies, including the Federal Deposit Insurance Corporation (FDIC), to conduct annual independent evaluations of their information security programs and practices and to report the results to the Office of Management and Budget (OMB). FISMA requires the independent evaluations 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. C&C planned and conducted its work based on the Department of Homeland Security's (DHS) reporting metrics: *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* Version 1.0.1, dated May 24, 2018 (the IG FISMA Reporting Metrics). OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency worked collaboratively and in consultation with the Federal Chief Information Officers (CIO) Council to develop the IG FISMA Reporting Metrics.

The IG FISMA Reporting Metrics require IGs to assess the effectiveness of their agencies' information security programs and practices on a maturity model spectrum. This maturity model aligns with the five function areas in the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*: Identify, Protect, Detect, Respond, and Recover. IGs must assign maturity level ratings to each of the five function areas, as well as an overall rating, using a scale of 1-5, where 5 represents the highest level of maturity. The five maturity model ratings are (1) Ad Hoc, (2) Defined, (3) Consistently Implemented, (4) Managed and Measurable, and (5) Optimized. In general, lower level maturity ratings (1-2) focus on defining policies, procedures, and strategies, while higher level ratings (4-5) focus on measuring and optimizing performance. According to the IG FISMA Reporting Metrics, maturity Levels 4 and 5 are considered to be effective levels of security at both the function and overall level.

Results

Applying the IG FISMA Reporting Metrics, C&C determined that the FDIC's overall information security program was operating at a maturity Level 3 (Consistently Implemented). According to the metrics, information security programs operating at

this level of maturity are not considered to be effective. The table below presents the maturity level ratings C&C assigned to each of the five function areas.

Function Area	Maturity Rating
Identify	1 (Ad hoc)
Protect	3 (Consistently Implemented)
Detect	2 (Defined)
Respond	3 (Consistently Implemented)
Recover	3 (Consistently Implemented)
Overall	**3 (Consistently Implemented)**

C&C found that the FDIC had established a number of information security program controls and practices that complied or were consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines. The FDIC also took or was working to take steps to strengthen its information security program controls following the FISMA audit conducted in 2017. For example, the FDIC established an agency-wide Incident Response Plan and updated its Breach Response Plan to address Federal policy requirements and guidelines; issued an *Information Security and Privacy Strategic Plan 2018 – 2021* that aligns with the *FDIC Information Technology Strategic Plan: 2017 – 2020*; and developed controls to help ensure the replacement or upgrade of software when vendors discontinue support.

However, 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. In many cases, these security control weaknesses were identified by other ongoing OIG audits, or through security control assessments completed by the FDIC. Although the FDIC was working to address these previously identified control weaknesses, the FDIC had not yet completed corrective actions at the time of this audit. Accordingly, these security control weaknesses continued to pose risk to the FDIC.

C&C's report contains sensitive information. Accordingly, we do not intend to make the report available to the public in its entirety. A brief description of the highest risk weaknesses that are appropriate for public release follows:

Information Security Risk Management (Identify). OMB and NIST have issued policy and guidance to help agencies implement enterprise risk management (ERM) programs to effectively manage the risks agencies face with respect to achieving their strategic objectives and arising from their activities and operations.

The FDIC was taking steps to align its risk management activities with OMB policy and NIST guidance. However, the FDIC had not fully defined or implemented an enterprise-wide and integrated approach to identifying, assessing, and addressing the full spectrum of internal and external risks, including those related to cybersecurity and the operation of information systems. Notably, the FDIC had not: completed efforts to revise its ERM program policy and procedures to define a holistic and integrated approach to risk management; updated its corporate risk inventory used to manage and prioritize risk mitigation activities; implemented an ERM Framework to improve decision making in governance, strategy, objective-setting, and day-to-day operations; or finalized and obtained senior management approval of a risk appetite, risk tolerance level, and risk profile.

The lack of an approved risk appetite, risk tolerance level, and risk profile limits the ability of FDIC Divisions and Offices to make effective risk management decisions. Further, the FDIC cannot be sure that it is effectively prioritizing resources toward addressing risks with the most significant potential impact on achieving strategic objectives.

Enterprise Security Architecture (Identify). The FISMA audit report issued in 2017 noted that the FDIC had not established a fundamental component of an effective information security program—an enterprise security architecture. According to NIST, an enterprise security architecture describes the structure and behavior of an organization's security processes, information security systems, and personnel and organizational subunits, and shows their alignment with the organization's mission and strategic plans. The previous FISMA audit report recommended that the FDIC develop an enterprise security architecture.

In July 2018, the FDIC provided an enterprise security architecture document, dated June 2018, that described the FDIC's information security planning, design, and governance processes and provided an overarching plan of action for change. The OIG plans to evaluate whether the enterprise security architecture document is responsive to the recommendation made in the FISMA report in 2017 as part of its audit follow-up process. The lack of an effective enterprise security architecture increased the risk that the FDIC's information systems would be developed with inconsistent security controls that are costly to maintain.

Security Control Assessments (Detect). FISMA requires agencies to test and evaluate their information security controls periodically to ensure they are effectively implemented. Based on separate OIG audit work, the OIG identified instances in which contractor-performed security control assessments did not include testing of security control implementation, when warranted. Instead, assessors relied on narrative descriptions of the controls in FDIC policies, procedures, and system

security plans and/or interviews of FDIC or contractor personnel. Without testing, assessors did not have a basis for concluding on the effectiveness of security controls. Inadequate FDIC oversight of security control assessments performed by contractor personnel contributed to this weakness.

The FDIC relies on the results of security control assessments to support a number of important risk management activities. These include identifying security weaknesses in the FDIC's information systems and information technology (IT) environment; prioritizing risk mitigation activities; confirming the resolution of known security weaknesses; informing security authorization decisions; and supporting resource allocation decisions. For these reasons, the FDIC must ensure that personnel perform security control assessments at an appropriate level of depth and coverage.

Patch Management (Protect). Software vendors release patches on a periodic or as-needed basis to address faults in operating systems or applications; alter functionality or address new security threats; or modify software configurations to make systems and applications less susceptible to attacks and more secure. Effective patch management is, therefore, critical to maintaining the confidentiality, integrity, and availability of the FDIC's IT infrastructure and the data that resides within it.

The FDIC's patch management processes were not always effective in ensuring that the FDIC implemented patches within FDIC-defined timeframes. In addition, the FDIC did not always follow its policy to create a Plan of Action and Milestones (POA&M) to address instances in which the FDIC did not install patches within required timeframes. Agency CIOs, security personnel, program officials, and others use POA&Ms as a risk management tool to track the progress of corrective actions pertaining to security vulnerabilities found in programs and information systems. Without POA&Ms, or another similar tracking and reporting mechanism, management may not devote an appropriate level of attention and resources to addressing overdue patches. Unpatched systems increase the risk of exposing the FDIC's network to a security incident.

Backup and Recovery (Recover). The FISMA audit report issued in 2017 noted that the FDIC's IT restoration capabilities were limited, and that the FDIC had 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. FISMA requires agencies to have plans and procedures for continuity of operations for information systems that support agency operations and assets. The FISMA audit report issued in 2017 recommended that the FDIC establish appropriate governance over its efforts to strengthen the resiliency and availability of its IT systems and applications.

In December 2017, the FDIC's Board of Directors authorized a multi-year Backup Data Center Migration Project designed to ensure that designated IT systems and applications supporting mission-essential functions can be recovered within targeted timeframes. As part of this project, the FDIC plans to migrate key IT systems and applications to a new and expanded backup data center in a different geographic location. Doing so will mitigate the current risk posed by the geographic proximity of the FDIC's backup data center to its primary data center. In addition, the new backup data center is intended to enhance security capabilities that are not available at the current recovery site.

In response to the recommendations made in the FISMA audit report in 2017, the FDIC established governance over this project. However, the FDIC will continue to have limited assurance that it can maintain and restore mission-essential functions within applicable timeframes during an emergency until the scheduled completion of the project in 2019.

Recommendations

C&C's report contains four new recommendations addressed to the CIO that are intended to improve the effectiveness of the FDIC's information security program and practices. These recommendations focus on improving controls in the areas of risk management, configuration management, and vulnerability scanning. As described in C&C's report, the FDIC was also working to implement an additional nine outstanding recommendations from prior FISMA audit reports.

In a written response to the report, the CIO Organization concurred with all four recommendations. The CIO Organization expects to complete actions to address the recommendations by June 28, 2019.