The FDIC's Information Security Program – 2022

September 2022 **AUD-22-004**

Audit Report

Audits, Evaluations, and Cyber

☆☆☆☆☆☆☆☆

REDACTED VERSION

PUBLICLY AVAILABLE

The redactions contained in this report are based upon requests from FDIC senior management to protect the Agency's information from disclosure.

Integrity*Independence*Accuracy*Objectivity*Accountability

Office of Inspector General

Executive Summary

The FDIC's Information Security Program – 2022

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 Assurance and Advisory, LLC (Cotton) to conduct this audit.

The objective of the audit was to evaluate the effectiveness of the FDIC's information security program and practices. Cotton planned and conducted its work based on OMB's Office of the Federal Chief Information Officer *Fiscal Year (FY) 2022 Core IG Metrics Implementation Analysis and Guidelines* (Department of Homeland Security [DHS] FISMA Reporting Metrics).

DHS FISMA Reporting Metrics require IGs to assess the effectiveness of their agencies' information security programs and practices using a maturity model. This maturity model is used to assess 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. In FY 2022, IGs were required to evaluate a subset of 20 "Core" FISMA metrics that represented a combination of OMB priorities and other critical controls. These Core metrics will continue to be tested each year, and the remaining metrics across the NIST Cybersecurity Function Areas will be evaluated on a two-year cycle beginning in FY 2023.

OMB and the Council of the Inspectors General on Integrity and Efficiency also adjusted the FISMA scoring system for FY 2022. IGs were required to assign maturity level ratings to each metric, as well as an overall rating, using a scale of 1-5, where 5 represents the highest level of maturity. The five maturity level ratings are (1) Ad Hoc, (2) Defined, (3) Consistently Implemented, (4) Managed and Measurable, and (5) Optimized.

The overall organizational information security program level for FY 2022 was determined by a simple majority where the most frequent level (mode) across the 20 metric questions served as the overall rating. This mode-based methodology may not fully capture the nature, scope, and magnitude of the risk posture of an agency's IT security, because it requires the agency to receive the higher rating

when there are an equal number of ratings at significantly different levels. As a result, an agency may still face significant risks even if its rating score is Managed and Measurable.

Results

Initially, we note that over the past year, the FDIC experienced several personnel changes in its leadership. For example, its Chief Innovation Officer and Chief Data Officer resigned from the Agency. In addition, the FDIC realigned the Chief Information Officer Organization's organizational structure, which resulted in the creation of two Deputy CIOs – one of whom is (b) (6) not currently serving in this role. The FDIC also made several changes to its IT infrastructure, including the acceleration of the use of cloud services.

With respect to the FISMA Core Metrics for FY 2022, Cotton determined that the FDIC's overall information security program was operating at a maturity level 4 (Managed and Measurable). In reaching this determination, Cotton was constrained by the methodology and limitations as required by the DHS FISMA Reporting Metrics. As discussed above, the mode-based scoring methodology employed by the DHS FISMA Reporting Metrics does not fully capture the risk posture of the agency's IT security. We caution the FDIC against complacency since deficiencies remain in the information security program at the FDIC.

This numerical score should not be compared to prior years, since the DHS FISMA Reporting Metrics have shifted over time. These changes, together with differences in the scope of audit work performed each year, make it imprudent to compare this year's maturity level ratings to prior year ratings.

The audit found that the FDIC had established a number of information security program controls and practices that were consistent with FISMA requirements, OMB policy and guidelines, and NIST security standards and guidelines. In addition, the FDIC completed certain actions to continue to strengthen its security controls since last year such as prioritizing the remediation of Plan of Actions and Milestones (POA&M); remediating outdated baseline configurations; and finalizing an Identity, Credential, and Access Management (ICAM) Roadmap.

However, the audit found security control weaknesses that reduced the effectiveness of the FDIC's information security program and practices. These control weaknesses can be improved to reduce the impact to the confidentiality, integrity, and availability of the FDIC's information systems and data. In many cases, these security control weaknesses were identified during OIG audits and evaluations that were either ongoing or completed, or through security and privacy control assessments completed by the FDIC. Because the FDIC has not yet completed the respective corrective actions, the following security control weaknesses continue to pose risk to the FDIC:

- **The FDIC's Supply Chain Risk Management (SCRM) Program Lacks Maturity:** The FDIC is still developing its policies and procedures to address the SCRM finding from the FISMA report for 2021. Additionally, we found, in our OIG evaluation report of the FDIC's SCRM program (issued March 2022) that the FDIC had not implemented several objectives outlined in its SCRM Implementation Project Charter; did not conduct supply chain risk assessments in accordance with best practices; had not ensured that its Enterprise Risk Management processes fully capture supply chain risks; and FDIC Contracting Officers did not maintain contract documents in the proper system. We issued nine recommendations, five of which remain unimplemented.
- **The FDIC Did Not Adequately Oversee and Monitor Information Systems:** The FDIC CIOO had not completed the authorization in accordance with the NIST Risk Management Framework for approximately 52 percent of its legacy systems and subsystems (as of May 19, 2022).
- **The FDIC Did Not Address Flaw Remediation Plan of Actions and Milestones (POA&M) in a Timely Manner:** The FDIC had 31 POA&Ms related to flaw remediation open past their estimated completion dates (as of June 21, 2022). These POA&Ms covered patch management, security updates for software products, system component flaws for the (b) (7)(E) General Support System, and outdated versions or unapplied security updates for several other applications and products.
- **The FDIC Did Not Configure Privileged Accounts in Accordance with the Principle of "Least Privilege":** We are currently conducting an audit of the FDIC's security controls over its Windows Active Directory. During the course of our work, we identified instances where accounts were configured with elevated account settings; however, there was no justification provided for such settings, and the elevated settings were no longer needed for administrators to perform their business roles. Additionally, we identified concerns relating to the Background Investigations for Privileged Account Holders at the FDIC and issued a Management Advisory Memorandum in June 2022.
- **The FDIC Did Not Fully Implement Its Document Labeling Guide:** In our FISMA report dated October 2021, we recommended that the FDIC implement document labeling guide requirements across the organization. However, the FDIC had not yet fully implemented this recommendation and did not anticipate implementation until later this year.

Finally, during the course of this audit, we learned that the FDIC process for emails included manual review by FDIC (FDIC employees and/or contractors) of messages flagged by automated tools. While not impacting the ratings of the core metrics, this process nevertheless presents potential security and privacy risks that FDIC employees and/or contractors could be inadvertently exposed to information that they would otherwise not be permitted to review. In addition, this process presents

risks that emails relevant to urgent law enforcement matters are not received by the OIG in a timely manner, thus presenting security and safety concerns. As a result, on July 11, 2022, the FDIC OIG issued a Memorandum to senior FDIC officials expressing our concerns regarding the FDIC's handling of OIG emails. The FDIC's CIOO responded that it intends to implement controls/infrastructure changes, and the FDIC OIG is currently working with Agency personnel to address these concerns.

Recommendations

The FISMA audit report contains one recommendation for the FDIC to address the 31 flaw remediation POA&Ms. Additionally, Appendix II contains a listing of unimplemented recommendations from prior FISMA reports, on which the FDIC should focus attention.

Contents

Part I

****

Report by Cotton & Company Assurance
and Advisory, LLC

THE FEDERAL DEPOSIT INSURANCE CORPORATION'S INFORMATION SECURITY PROGRAM – 2022

AUDIT REPORT

SEPTEMBER 26, 2022

Cotton, A Sikich Company
333 John Carlyle Street, Suite 500
Alexandria, Virginia 22314
703.836.6701 | 703.836.0941, fax
lschwartz@cottoncpa.com | www.cottoncpa.com

TABLE OF CONTENTS

Cotton
A SIKICH. COMPANY

333 John Carlyle Street, Suite 500 | Alexandria, VA 22314
P: 703.836.6701 | F: 703.836.0941 | www.cottoncpa.com

Jason M. Yovich
Deputy Assistant Inspector General for Audits, Evaluations, and Cyber
Office of Inspector General
Federal Deposit Insurance Corporation

Subject: Audit of the Federal Deposit Insurance Corporation's Information Security Program – 2022

Cotton & Company Assurance and Advisory, LLC (Cotton) is pleased to submit the attached report detailing the results of our performance audit of the Federal Deposit Insurance Corporation's (FDIC) information security program. 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. FISMA states that the evaluations are to be performed by the agency Inspector General (IG), or by an independent external auditor as determined by the IG. The FDIC Office of Inspector General engaged Cotton to conduct this performance audit. Cotton performed the work from March through July 2022.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards promulgated by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Sincerely,

(b) (6)

Loren Schwartz CPA, CISSP, CISA
Partner

INTRODUCTION

According to the Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA), the United States faces persistent and increasingly sophisticated cyber attacks that affect the security and privacy of the public sector, private sector, and the American people. CISA urges the Federal Government to aggressively remediate known exploited vulnerabilities to protect federal information systems. Of the more than 160,000 vulnerabilities in the National Institute of Standards and Technology (NIST) National Vulnerability Database, fewer than 4 percent have been publicly exploited. However, of those exploited, 42 percent were used by attackers on the first day of disclosure; 50 percent by the second day; and 75 percent by the end of the first month (28th day after disclosure).[1]

Notably, in December 2021, a critical exploited vulnerability was found in the Apache Log4j tool,[2] which is broadly used in consumer and enterprise services, applications, and websites. This vulnerability can be exploited remotely to take control of an affected information system, serving as a reminder that the Federal Government must continually invest in capabilities to reduce the impact of cybersecurity incidents.

The Federal Deposit Insurance Corporation (FDIC) relies heavily on information systems to carry out its responsibilities of insuring deposits; examining and supervising financial institutions for safety, soundness, and consumer protection; making large and complex financial institutions resolvable; and managing receiverships. These systems contain sensitive information, such as Personally Identifiable Information (PII), including names, Social Security Numbers, and bank account numbers for FDIC employees and depositors of failed financial institutions; confidential bank examination information, including supervisory ratings; and sensitive financial data, including credit card numbers. Without effective controls for safeguarding its information systems and data, the FDIC would be at increased risk of a cyberattack that could disrupt critical operations and allow inappropriate access to, and disclosure, modification, or destruction of, sensitive information. Such an attack could threaten the FDIC's ability to accomplish its mission of ensuring the safety and soundness of institutions and maintaining stability in our Nation's financial system.

The Federal Information Security Modernization Act of 2014 (FISMA)[3] requires Federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. FISMA directs NIST to develop risk-based standards and guidelines to assist agencies in defining security requirements for their information and information systems. NIST develops and communicates required security standards within Federal Information Processing Standards (FIPS) publications and recommended guidelines within NIST Special Publications (SP). NIST SPs provide Federal agencies with a framework for developing appropriate controls over confidentiality, integrity, and availability for their information and information systems.

---

[1] CISA's Binding Operational Directive 22-01 *Reducing the Significant Risk of Known Exploited Vulnerabilities* establishes requirements for agencies to remediate any vulnerabilities included in the CISA-managed known exploitable vulnerabilities catalog. See https://www.cisa.gov/binding-operational-directive-22-01 for details.
[2] *See* Apache Log4j Vulnerability Guidance https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance for details.
[3] Pub. L. No. 113-283 (December 2014). FISMA's obligations for Federal agencies and for Federal Inspectors General, as relevant to this audit, are codified chiefly to 44 U.S.C. §§ 3554 and 3555, respectively. The FDIC has determined that FISMA is legally binding on the FDIC.

On February 12, 2014, NIST published the *Framework for Improving Critical Infrastructure Cybersecurity* (NIST Cybersecurity Framework). NIST subsequently updated the framework on April 16, 2018. The NIST Cybersecurity Framework:

- Contains a set of industry standards and best practices to help organizations manage their cybersecurity risks;
- Focuses on using business drivers to guide cybersecurity activities and consider cybersecurity risks as part of the organization's risk management processes; and
- Enables organizations, regardless of size, degree of cybersecurity risk, or cybersecurity sophistication, to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure.

Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 2017),[4] requires Federal agencies to use the NIST Cybersecurity Framework to manage their cybersecurity risks. We used the NIST Cybersecurity Framework when assessing the effectiveness of the FDIC's information security program.

The Office of Management and Budget (OMB) also issues information security policies and guidelines for Federal information resources pursuant to various statutory authorities. Further, DHS serves as the operational lead for Federal cybersecurity. DHS has the authority to coordinate Government-wide cybersecurity efforts and issue binding operational directives detailing actions that Federal agencies must take to improve their cybersecurity posture. Further, DHS provides operational and technical assistance to agencies and facilitates information sharing across the Federal Government and the private sector.

AUDIT OBJECTIVE

The objective of this performance audit was to evaluate the effectiveness of the FDIC's information security program and practices. We considered FISMA requirements, NIST security standards and guidelines, the NIST Cybersecurity Framework, OMB policy and guidance, FDIC policies and procedures, and DHS guidance and reporting requirements to plan and perform our work and to conclude on our audit objective. **Appendix I** contains more information about our scope and methodology to achieve the objective.

DHS FISMA REPORTING METRICS AND THE NIST CYBERSECURITY FRAMEWORK

OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) worked collaboratively and in consultation with the Federal Chief Information Officers (CIO) Council to develop the OMB Office of the Federal Chief Information Officer *Fiscal Year (FY) 2022 Core IG Metrics Implementation Analysis and Guidelines* (DHS FISMA Reporting Metrics). The DHS FISMA Reporting Metrics align with the five function areas defined in the NIST Cybersecurity Framework: *Identify*, *Protect*, *Detect*, *Respond*, and *Recover*. These function areas organize basic cybersecurity activities at a

[4] The FDIC has determined that portions of Executive Order 13800 are not legally binding on the FDIC. However, the FDIC has determined that it should comply with those provisions that are similar to FISMA requirements and pertain to agency risk management reporting. The FDIC is voluntarily complying with provisions of Executive Order 13800 related to the NIST Cybersecurity Framework.

high level. Aligning the DHS FISMA Reporting Metrics with the NIST Cybersecurity Framework ensures that Inspectors General (IG) evaluate agency information security programs using the same framework that agencies are required to use to manage their cybersecurity risks. This alignment provides agencies with a meaningful independent assessment of the effectiveness of their information security programs and promotes consistency among IG FISMA evaluations. The DHS FISMA Reporting Metrics divide the five function areas into nine domains. Table 1 below illustrates the alignment of the function areas with the domains.

Table 1: Alignment of the NIST Cybersecurity Framework Function Areas with the DHS FISMA Reporting Metric Domains

Function Area	Function Area Objective	Domain(s)
Identify	Develop an organizational understanding of the business context and the resources that support critical functions to manage cybersecurity risk to systems, people, assets, data, and capabilities.	**Risk Management and Supply Chain Risk Management**
Protect	Implement safeguards to ensure delivery of critical infrastructure services, as well as to prevent, limit, or contain the impact of a cybersecurity event.	**Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training**
Detect	Implement activities to identify the occurrence of cybersecurity events.	**Information Security Continuous Monitoring (ISCM)**
Respond	Implement processes to take action regarding a detected cybersecurity event.	**Incident Response**
Recover	Implement plans for resilience to restore any capabilities impaired by a cybersecurity event.	**Contingency Planning**

Source: Cotton's analysis of the NIST Cybersecurity Framework and DHS FISMA Reporting Metrics.

The DHS FISMA Reporting Metrics require IGs to assess the effectiveness of their agency's information security program and practices using a maturity model. Figure 1 describes the five levels of the maturity model: *Ad Hoc*, *Defined*, *Consistently Implemented*, *Managed and Measurable*, and *Optimized*. Maturity Level 1 (*Ad Hoc*) and Level 2 (*Defined*) are considered foundational, while Maturity Level 4 (*Managed and Measurable*) and Level 5 (*Optimized*) are considered advanced. According to the DHS FISMA Reporting Metrics, the foundational maturity levels ensure that agencies develop sound policies and procedures, and the advanced levels capture the extent to which agencies institutionalize those policies and procedures. Maturity Level 3 (*Consistently Implemented*) indicates that the organization has policies and procedures in place but must strengthen its quantitative and qualitative effectiveness measures for its security controls. Within the context of the maturity model, a Maturity Level 4 (*Managed and Measurable*) information security program is considered to be operating at an effective level of security.[5]

[5] Information regarding the determination of maturity level ratings can be found at https://www.cisa.gov/federal-information-security-modernization-act#.

Figure 1: FISMA Maturity Model Levels

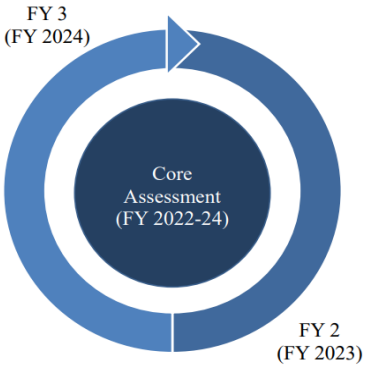
Source: DHS FISMA Reporting Metrics.

Ratings for the overall information security program are determined by the most frequent level (mode) across all the metrics. For example, if the agency receives Level 1 ratings for nine component questions and Level 5 ratings for 11 component questions, then the DHS FISMA Reporting Metrics requires that the overall rating be at a Level 5 (Optimized) – even though nine ratings were at an Ad Hoc level (Level 1) and represented significant weaknesses in the information technology (IT) security system. If there is a tie for the most frequent rating, the agency will be rated at the higher level. As a result, an agency may receive a rating such as "Managed and Measurable" or "Optimized" even though weaknesses exist in its IT security environment.

Changes to DHS FISMA Reporting Metrics

OMB Memorandum M-22-05 – *Fiscal Year 2021 – 2022 Guidance on Federal Information Security and Privacy Management Requirements* – detailed changes to the scope and schedule of the annual IG FISMA submission. In FY 2021, IGs were required to assess 66 metrics annually and submit their results at the end of October. In FY 2022, OMB and CIGIE shifted the evaluation process to a multi-year cycle beginning in FY 2022.

Figure 2: FISMA Assessment Schedule



Source: OMB Memo M-22-05

Within this cycle, in FY 2022, IGs were required to evaluate a subset of 20 FISMA metrics that represent a combination of OMB priorities and other critical controls, on an annual basis. These 20 metrics are the "Core" metrics and will continue to be tested each year. The remaining metrics across the NIST Cybersecurity Function Area and Domains will be divided up and evaluated on a 2-year cycle beginning in FY 2023. Therefore, in FY 2023, the second year of the cycle, IGs will be required

to assess both the 20 Core metrics and half the remaining 46 metrics. See Figure 2 for a graphical representation of the new cycle.

OMB and CIGIE also adjusted the FISMA scoring system. In FY 2022, the organizational information security program level is the most common metric rating (mode) across the 20 core metrics, without regard to the Function Area and Domain ratings.

Lastly, OMB shifted the due date of the metrics from October to July. This change was intended to align the IG assessments with the development of the President's Budget, and it allows each agency to request funding to remediate findings in a timely manner.

Zero Trust Architecture

M-22-05 identified "Moving to a Zero Trust Architecture" as a key tenet to guide continued reforms under FISMA. OMB Memorandum M-22-09 – *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (dated January 26, 2022) – defined the Zero Trust Architecture Model as an environment in which "*no actor, system, network, or service operating outside or within the security perimeter is trusted*." Memorandum 22-09 defines five security objectives – Identity, Devices, Networks, Applications and Workloads, and Data – that support CISA's Zero Trust Architecture Model:

- **Identity**: Federal staff have enterprise-managed accounts, allowing them to access applications while remaining reliably protected from targeted, sophisticated phishing attacks.
- **Devices**: The devices of Federal staff are consistently tracked and monitored, and the security posture of these devices is taken into account when granting access.
- **Networks**: Agency systems are isolated from each other, and the network traffic flowing between and within them is reliably encrypted.
- **Applications and Workloads**: Enterprise applications are tested internally and externally, and can be made available to staff securely over the internet.
- **Data**: Federal security teams and data teams work together to develop data categories and security rules to automatically detect and ultimately block unauthorized access to sensitive information.

OMB Memorandum M-22-09 requires agencies to achieve the objectives by the end of FY 2024. By the end of FY 2022 (September 30, 2022), agencies have two primary requirements:

1. Designate an implementation lead; and
2. Draft and submit a Zero Trust Implementation Plan.

Certain DHS FISMA Reporting Metrics cover control activities supporting each of the five pillars. DHS has mapped several Core Metrics to OMB Memorandum M-22-09. For example, one Core Metric in the Identify function area evaluates the organization's adoption of authentication mechanisms, which is relevant to the Identity pillar. Therefore, in addition to assessing the FDIC's current efforts to transition to a Zero Trust Architecture Model in compliance with M-22-09 requirements, we also tested controls relevant to Zero Trust Architecture Model during our assessment of the Core Metrics. As of May 2022, the FDIC had taken the following actions related to Zero Trust Architecture Model:

- Submitted a Zero Trust Implementation Plan to OMB in accordance with M-22-09.

- Developed a Zero Trust Near Term Strategy consisting of five steps, which may lead to a long-term strategy.
- The FDIC designated an implementation lead and assembled a Core Team and Zero Trust Task Force responsible for implementation.
- Defined a Zero Trust Maturity Model leveraging guidance from the Department of Defense (DOD) and NIST.

Endpoint Detection and Response

EO 14028 on *Improving the Nation's Cybersecurity* (May 12, 2021) directed OMB to issue requirements for adopting Endpoint Detection and Response (EDR) solutions. Accordingly, OMB issued Memorandum M-22-01 *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* (October 8, 2021) to provide guidance to agencies as they accelerate the adoption of EDR solutions. EDR combines real-time continuous monitoring and collection of endpoint data with automated rules-based response and analysis, providing the increased visibility needed to respond to advanced cybersecurity threats.

OMB Memorandum M-22-01 requires agencies to achieve certain objectives by February 11, 2022. The primary requirements are:

1. Provide CISA personnel with access to their solution to enable support of the Federal Government-wide EDR initiative; and
2. Conduct a gap analysis of their EDR capabilities in coordination with CISA.

As of February 1, 2022, the FDIC had taken the following actions related to adopting an EDR solution:

- Provided CISA with access to their solution (b) (7)(E) .
- Conducted a gap analysis of their EDR capabilities. CISA did not identify gaps in the FDIC's current EDR solution when compared to the requirements defined in OMB Memorandum M-22-01 and EO 14028.

Supply Chain Risk Management

The risks in the Federal Government's supply chain were acknowledged in the Federal Acquisition Supply Chain Security Act of 2018,[6] which directed agencies to assess, avoid, mitigate, accept, or transfer supply chain risks. Subsequently, the FY 2021 DHS FISMA Reporting Metrics introduced the Supply Chain Risk Management (SCRM) Domain within the Identify Function. The Domain references SCRM criteria newly defined in NIST SP 800-53 Rev. 5 *Security and Privacy Controls for Information Systems and Organizations* (September 23, 2020). The SCRM Domain highlights the dependence on products, systems, and services from external providers that present additional risks to an organization. These risks include:

- The insertion or use of counterfeits.
- Tampering with software and hardware.
- The insertion of malicious software and hardware.

[6] The Federal Acquisition Supply Chain Act of 2018, Title II of the SECURE Technology Act, Public Law 115-390 (2018).

- Poor manufacturing and development practices in the supply chain.

Metrics in the SCRM Domain were not included in the overall score in the previous year (2021). This year (2022), SCRM metrics are included in the calculation of the organization's overall score. As of June 2022, the FDIC is operating at a Level 1 (Ad Hoc) maturity level for the SCRM Domain.

OVERVIEW OF THE FDIC'S INFORMATION SECURITY PROGRAM

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Agency heads are also responsible for complying with the requirements of FISMA and related policies, procedures, standards, and guidelines. For purposes of FISMA, the FDIC Chairman is the agency head.

The FDIC Chairman has delegated the authority to ensure compliance with FISMA to the FDIC's CIO. The CIO reports directly to the FDIC Chairman and has broad strategic responsibility for IT governance, investments, program management, and information security. The CIO also serves as the Chief Privacy Officer (CPO)[7] and the Director of the Division of Information Technology (DIT). As the CPO, which is a statutorily mandated position, the CIO is designated as the Senior Agency Official for Privacy (SAOP), responsible for establishing and implementing a wide range of privacy and data protection policies and procedures pursuant to legislative and regulatory requirements. As the Director of the DIT, the CIO also has overall responsibility for IT operations.

On February 28, 2022, CIO Organization (CIOO) announced that the FDIC was realigning FDITECH within the CIOO. FDICTECH is an FDIC organization that promotes technology innovation and is led by a Chief Innovation Officer (CINO). As of August 15, 2022, this role is filled in an acting capacity. The FDITECH is comprised of permanent staff and FDIC employees on detail with various areas of expertise. Operationally, FDITECH identifies technology projects based on emerging technology and technology needs.

The FDIC's Chief Information Security Officer (CISO), who reports directly to the CIO, is delegated responsibility for establishing an agency-wide information security vision and strategy, including the creation and maintenance of the FDIC's information security and privacy policy, risk assessment, compliance, and oversight. The CISO oversees a group of IT security professionals within the Office of the CISO (OCISO), which is part of the CIOO. The mission of the OCISO is to develop and maintain agency-wide information security and privacy programs that support the mission of the FDIC.

FDIC Divisions and Offices also play an important role in securing information and information systems. Each Division/Office within the FDIC appoints an Information Security Manager (ISM) to assist with general information security related functions. ISMs also serve as the liaison between the Division/Office and OCISO security personnel. In addition, the ISMs are responsible for facilitating information security activities for contractor systems utilized within their Office/Division.

[7] *See* Consolidated Appropriations Act of 2005, div. H, sec. 522, Pub. L. No. 108-447, 118 Stat. 3268 (codified as amended at 42 U.S.C. § 2000ee-2).

To effectively secure and safeguard the Corporation's information and information systems, and to enhance FISMA compliance, the FDIC has assigned Information Systems Security Managers (ISSMs) to systems owned by the Division of Risk Management Supervision (RMS), Division of Resolutions and Receiverships (DRR), Division of Depositor and Consumer Protection (DCP), Division of Insurance and Research (DIR), Division of Complex Institution Supervision & Resolution (CISR), Division of Finance (DOF), Division of Administration (DOA), Legal Division (Legal), Office of Communications (OCOM), Executive Offices, and the CIOO. Working under the direction of OCISO, the ISSMs are responsible for working with key stakeholders (i.e. Systems Owners, Project Managers, Divisional/Office Information ISMs) for integrating and managing NIST Risk Management Framework (RMF) tasks and activities for systems within their assigned portfolios.

SUMMARY OF RESULTS

Based on the results of our audit work and the application of the DHS FISMA Reporting Metrics, we determined that the FDIC's information security program is operating at a Maturity Level 4 (*Managed and Measurable*). Achieving Level 4 does not mean that the FDIC is without risks to cyberattack. As described in our audit results, there are deficiencies which remain at the FDIC. Tables 2 and 3 provide a breakdown of the maturity level ratings that led us to conclude upon the rating of the FDIC's overall information security program.

This numerical score should not be compared to prior or future years. The DHS FISMA Reporting Metrics undergo changes – sometimes significant – annually, with this year's Metrics serving as the prime example of the potential scope of year-over-year changes. These changes, together with anticipated differences in the scope of audit work performed in subsequent years, make it imprudent to compare this year's maturity level ratings to ratings in both prior and future years.

Table 2: Maturity Level Ratings by Metric

Function	Domain	Metric Description	Metric Maturity Level Rating
Identify	Risk Management	System Inventory	4
		Hardware Asset Management	4
		Software Asset Management	4
		Cybersecurity Risk Management	5
		Cybersecurity Risk Portfolio	5
	Supply Chain Risk Management	Cybersecurity and Supply Chain Requirements and Compliance	1
Protect	Configuration Management	Security Configuration Settings	4
		Patch and Vulnerability Management	2
	Identity and Access Management	Non-Privileged Authentication	4
		Privileged Authentication	4
		Privileged Account Management	2
	Data Protection and Privacy	Safeguarding PII and Sensitive Information	2

Function	Domain	Metric Description	Metric Maturity Level Rating
		Data Exfiltration and Network Defense	3
	Security Training	Workforce Skills Assessment	4
Detect	ISCM	ISCM Strategy	3
		Continuous Assessments and Authorizations	2
Respond	Incident Response	Incident Detection and Analysis	4
		Incident Handling and Containment	4
Recover	Contingency Planning	Business Impact Analysis	4
		Contingency Plan Testing	4

Source: Cotton's assessment of the FDIC's information security program controls and practices based on the DHS FISMA Reporting Metrics.

Note: Consistent with the historical guidance in the DHS FISMA Reporting Metrics, we determined maturity ratings using a simple majority (or mode) where the most frequent rating across the 20 core metrics determined overall program maturity rating.

We found that the FDIC established a number of information security program controls and practices that were consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines. The FDIC also took action to strengthen its security controls following the issuance of our FISMA audit report in October 2021. For example, the FDIC:

- Prioritized the remediation of Plan of Actions and Milestones (POA&M) and enhanced communication between POA&M testers and POA&M owners during the closure process.
- Implemented physical walkthroughs of facilities and scans of network shared folders to systematically detect and safeguard sensitive information and PII.
- Remediated outdated baseline configurations using current security benchmarks listed in the NIST National Checklist Program (NCP) Repository.
- Finalized an Identity, Credential, and Access Management (ICAM) Roadmap and began tracking the progress of the 11 Roadmap initiatives planned for completion by December 31, 2022.
- Performed required Privacy Impact Assessments (PIA) and posted the PIAs on its public website.
- Conducted security control assessments for its cloud-based systems.
- Enhanced processes to ensure Confidentiality Agreements for contractor and subcontractor personnel are executed and maintained.
- Updated its annual security training to address mobile device risks.
- Developed privacy plans for systems containing PII.
- Refreshed documentation to reflect the current organizational structure of the Privacy Program and responsibilities of associated personnel and offices.

Notwithstanding these actions, our report describes security control weaknesses that reduced the effectiveness of the FDIC's information security program and practices. The FDIC can reduce the impact of these weaknesses by improving the confidentiality, integrity, and availability[8] of its information systems and data. In many cases, these security control weaknesses were identified during Office of Inspector General (OIG) audits and evaluations, or through security and privacy control assessments completed by the FDIC. These unaddressed audit and evaluation findings represent security control weaknesses that continue to pose risk to the FDIC. The security control weaknesses we identified include:

- The FDIC's Supply Chain Risk Management Program Lacks Maturity
- The FDIC Did Not Adequately Oversee and Monitor Information Systems
- The FDIC Did Not Remediate Certain POA&MS in a Timely Manner
- The FDIC Did Not Configure Privileged Accounts in Accordance with Least Privilege
- The FDIC Has Not Implemented Its Document Labeling Guide

In addition, **Appendix II** contains the status of recommendations made in prior year FISMA audit reports.

AUDIT RESULTS

The following section of the report describes the key controls underlying each Domain and our assessment of the FDIC's implementation of those controls. We are organizing our conclusions and ratings by Function Area and Domain to help orient the reader to deficiencies as categorized by the NIST Cybersecurity Framework.

IDENTIFY

The objective of the *Identify* Function is to develop an organizational understanding of how to manage cybersecurity risks to agency systems, assets, data, and capabilities.

Risk Management

The *Risk Management* Domain includes controls that address an agency's maturity in the management of cybersecurity risks.

The FDIC had implemented processes for maintaining a comprehensive and accurate inventory of information systems, hardware, software, and software licenses. We also noted that the FDIC had completed a Risk Inventory and Risk Profile[9] to document, categorize, and track risks. We also found that the FDIC used an automated tool to centralize the management of these risk processes across the organization. Further, the FDIC's IT Risk Advisory Council (ITRAC)[10] monitored IT and cybersecurity risks

[8] NIST SP 800-12, *An Introduction to Information Security* defines information security as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability. The effectiveness of these three elements – confidentiality, integrity, and availability – determines the effectiveness of an organization's information security.
[9] The FDIC defines a *Risk Profile* as a prioritized list of the most significant risks identified and assessed through the risk assessment process.
[10] The ITRAC is comprised of the CIO, CISO, Chief Risk Officer, and other FDIC stakeholders.

facing the FDIC to determine whether they were within established Risk Tolerance levels and the FDIC's Risk Appetite.

The FDIC also completed corrective actions for an outstanding audit recommendation issued in the FISMA report for 2016 related to the FDIC's large backlog of POA&Ms for the Data Communications (DCOM) system. The agency did so by increasing management prioritization of the POA&M backlog and developing communication protocols between POA&M owners and reviewers to determine whether to close a POA&M. The OIG closed this recommendation.

Supply Chain Risk Management

The *Supply Chain Risk Management* Domain includes controls that address an agency's maturity in a range of activities related to the supply chain management of cybersecurity risks. We tested FDIC's processes to ensure that external providers adhere to the FDIC's cybersecurity and SCRM requirements.

The FDIC's Supply Chain Risk Management Program Lacks Maturity

In the FISMA report for 2021, we issued a recommendation to develop and implement processes and procedures required by FDIC Directive 3720.01, *Supply Chain Risk Management Program,* published in June 2021. Since then, the FDIC has:

- Engaged an SCRM team that includes the OCISO, CIOO, Office of Risk Management & Internal Controls (ORMIC), DOA, Legal, RMS, DRR, CISR, DCP, and DIR.
- Published an SCRM Strategy containing five high-level objectives.
- Performed an analysis of supply chain threat scenarios as defined by the CISA.[11]
- Modified its acquisition process to include an OCISO review of security and privacy requirements for all acquisitions; and
- Began drafting an SCRM Implementation Plan to support the execution of its strategic objectives defined in the SCRM Strategy.

However, the FDIC is still developing its policies and procedures to address the SCRM finding from the FISMA report for 2021.

In March 2022, the OIG completed an Evaluation on the FDIC's Implementation of SCRM[12] and found that the FDIC had not implemented several of its defined SCRM objectives, identified or documented its SCRM risks, or established metrics and indicators for SCRM. The OIG issued nine recommendations that direct the FDIC to identify, document, and monitor supply chain risks and conduct supply chain risk assessments. Further, the OIG recommended the FDIC's Enterprise Risk Management Program articulate the extent and significance of supply chain risks. As of August 1, 2022, the following five recommendations remain open:

- Develop metrics and indicators for gauging and monitoring supply chain risk;

[11] CISA *Supplier, Products, and Services Threat Evaluation* Report, July 2021.
https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v3.pdf
[12] FDIC OIG Report, *The FDIC's Implementation of Supply Chain Risk Management*, March 2022
https://www.fdicoig.gov/sites/default/files/publications/EVAL-22-003-Corrected.pdf

- Implement SCRM controls during the IT procurement process;
- Define a risk-based process for considering supply chain risks in procurement actions;
- Apply a risk-based process for considering supply chain risks when entering into new contracts; and
- Apply a risk-based process for considering supply chain risks when contracts are renewed, extended, or have option periods exercised.

The FDIC stated that it will complete corrective actions for these recommendations by November 30, 2022.

Visibility into supply chain activities is important for monitoring and identifying high-risk threats and events associated with using external vendors. The FDIC's use of third-party services may require it to trust and provide resource access to those third parties. Without effective SCRM controls, it is easier for an adversary to leverage weak third-party controls to access the FDIC environment, interfere with Agency operations, or exploit information for their own benefit. Without increased visibility into its supply chains and the associated risks, the FDIC's ability to identify supply chain vulnerabilities consistently, and to evaluate, monitor, and address risks effectively, is limited.

PROTECT

The objective of the *Protect* Function is to develop and implement safeguards to secure information systems by preventing, limiting, or containing the impact of a cybersecurity event.

Configuration Management

The *Configuration Management* Domain includes controls that address an agency's maturity in ensuring the integrity, security, and reliability of any information system by requiring disciplined processes for managing the changes that occur to the system during its life cycle.

The FDIC had established policies and implemented processes for baseline configurations and patch management.[13] The FDIC also completed actions to address an earlier recommendation from the FISMA report for 2020 related to incomplete and outdated baseline configurations for IT systems.[14] The FDIC addressed these issues by revising 13 baseline configurations to reflect current security benchmarks listed in the NIST NCP repository.[15] The OIG closed this recommendation.

However, the FDIC had not taken sufficient action to close 31 POA&Ms created to track the remediation of certain vulnerabilities that were non-compliant with the organizational policy on patching.

The FDIC Did Not Remediate Certain POA&MS in a Timely Manner

The FDIC's CIOO Policy No. 19-005, *Security Patch Management,* addresses the FDIC's handling of software security patches. This policy states that patching and vulnerability remediation activities will

[13] Such policies included CIOO Policy No. 19-005, *Policy on Security Patch Management* (April 2019); and CIOO Policy No. 16-005, *Policy on Secure Baseline Configuration Guides* (June 2021).
[14] This recommendation is listed in Appendix II as Recommendation 3 from the FISMA audit report issued in 2020.
[15] The National Checklist Program (NCP) is the U.S. government repository of publicly available security checklists that provide detailed low-level guidance on setting the security configuration of operating systems and applications. The checklist is located at https://ncp.nist.gov/repository.

be prioritized based on factors such as the vulnerability score, FDIC mission impact, business constraints, exploitability, schedule, threat intelligence, and availability. The FDIC should remediate vulnerabilities within the timeframes defined by the FDIC's security patching schedule. Where the FDIC does not apply actions within the specified timeframes in the FDIC's patching schedule, such vulnerabilities are converted to create a POA&M. The FDIC should assign POA&Ms to a completion schedule in accordance with the risk-based criteria defined in the FDIC's *POA&M and Acceptance of Risk Process* document.

The FDIC had mechanisms to ensure that the most critical patches, including emergency patches like those communicated in CISA alerts,[16] were tracked and remediated in a timely manner. The FDIC also demonstrated high patching compliance for platforms across the organization.

However, as of June 21, 2022, the FDIC had 31 POA&Ms open past their estimated completion date. These POA&Ms related to vulnerabilities that were non-compliant with the organizational patch management policy and they pertained to security updates for (b) (7)(E) products, system component flaws for the (b) (7)(E) General Support System (GSS), and outdated versions or unapplied security updates for several other applications and products. The FDIC has commenced a risk acceptance process for eleven of these POA&Ms.

The estimated completion dates for POA&Ms without a risk acceptance ranged from December 2019 to March 2022. We identified 14 notable examples of open POA&Ms without a risk acceptance:

- Nine POA&Ms related to unapplied security updates for (b) (7)(E) [17] products.
- One POA&M related to a security configuration setting that is misaligned with defined baseline requirements for (b) (7)(E) .
- Two POA&Ms related to outdated versions of (b) (7)(E) [18] web servers that are susceptible to denial of service and privilege escalation attacks.
- Two POA&Ms related to outdated versions of the (b) (7)(E) [19] that makes applications susceptible to remote code execution and reflected file download vulnerabilities. These applications include the (b) (7)(E) These systems are used to manage identity and access for FDIC systems, store bank closing records and resolution plans for financial institutions, and facilitate the creation and monitoring of procurement activities and artifacts throughout the acquisition lifestyle, respectively.

Patches and updates are intended to fix known system vulnerabilities; however, they rely on customers, such as the FDIC, to implement them. If the FDIC does not timely update its systems, it increases the risk that attackers will be able to use publicly known vulnerabilities to deny legitimate users' access to FDIC systems or obtain unauthorized access to and modify FDIC data.

---

[16] The FDIC's vulnerability management processes enabled the effective handling of flaws identified in (b) (7)(E) . A Common Vulnerability and Exposure (CVE) is database of publicly known vulnerabilities.

[17] (b) (7)(E)

[18] (b) (7)(E) s.

[19] (b) (7)(E)

Recommendation

We recommend that the CIO:

1. Address the 31 POA&Ms identified as of June 21, 2022, associated with NIST SP 800-53 Rev. 5 control SI-2 (Flaw Remediation).

Identity and Access Management

The *Identity and Access Management* Domain includes controls that address an agency's maturity in implementing a set of capabilities to ensure that only authorized users, processes, and devices have access to the organization's IT resources and facilities, and that their access is limited to the minimum necessary to perform their jobs.

The FDIC had developed policies and procedures for identifying, authenticating, and managing users who access FDIC information systems and facilities. [20] The FDIC also completed corrective actions for an outstanding recommendation issued in the FISMA report for 2020 related to the FDIC's sizeable backlog of POA&Ms related to administrative access. Finally, the FDIC completed corrective actions for an outstanding recommendation issued in the FISMA report for 2021 related to the FDIC not tracking the completion of its ICAM Roadmap initiatives. The OIG closed these recommendations.

However, the FDIC's management of privileged accounts still needed improvement.

The FDIC Did Not Configure Privileged Accounts in Accordance with Least Privilege

The effective implementation of identity and access management controls is particularly important for Administrative Accounts within networks and information systems. Administrative Accounts have elevated access privileges that can bypass system controls and access sensitive system resources. For these reasons, Administrative Accounts are highly sought-after targets by hackers and other adversaries to use the accounts to corrupt data, launch attacks, or conduct other malicious activities. As a result, Administrative Accounts must be carefully provisioned, monitored, and deactivated when no longer necessary.

The FDIC uses a directory service called Active Directory (AD) to manage user privileges across the organization. The FDIC employs a Role-Based Access Control (RBAC) system in which it defines a list of roles, each with a set of system permissions, that are configured in AD. FDIC users who need system access are given one or more roles in accordance with their business need. Privileged accounts are defined as such because they hold multiple roles that are considered privileged.

The OIG is currently working on an audit related to the FDIC's Security Controls Over Microsoft Windows AD. The objective of this audit is to assess whether the FDIC designed and implemented effective controls for the AD to protect network systems and data. The OIG identified instances where accounts

[20] Such policies and procedures include, but are not limited to: FDIC Directives 1360.1, *Automated Information Systems (AIS) Security Program* (March 2011); 1600.8, *Personal Identity Verification (PIV) Card Program* (July 2017); and 1610.2, *Personnel Security and Suitability Program for Contractors and Contractor Personnel* (January 2020).

were configured with elevated account settings; however, there was no justification provided for such settings, and the elevated settings were no longer needed for administrators to perform their business roles. Potential attackers seeking to gain access to FDIC system resources could exploit these settings and gain privileged access within the FDIC network, allowing them to access, control, or destroy elements of the FDIC's IT infrastructure and the applications it supports. We encourage FDIC Management to take prompt corrective action to address weaknesses identified in the AD audit upon its report issuance.

Additionally, on June 22, 2022, the OIG issued a Management Advisory Memorandum identifying concerns relating to Background Investigations for Privileged Account Holders.[21] The Memorandum stated that the FDIC does not have adequate controls to ensure certain contractors and employees who require privileged access to FDIC information systems and data have background investigations commensurate with appropriate determinations of risk. The FDIC acknowledged the need to improve procedures to ensure that its personnel have the correct background investigations, especially when their access privileges increase.

Data Protection and Privacy

The *Data Protection and Privacy* Domain includes controls that address an agency's maturity in implementing a privacy program to properly collect, use, maintain, protect, share, and dispose of PII.

The FDIC had issued a Document Labeling Directive that establishes requirements for categorizing and labeling documents. The FDIC also employed mechanisms, such as firewalls, email authentication technology, and a Data Loss Prevention (DLP) tool, to detect and minimize exfiltration of information, including PII. The FDIC also completed corrective actions for multiple audit recommendations associated with its Privacy Program:

- The FISMA report for 2021 noted that the FDIC had not completed PIAs for all required systems. In 2022, the FDIC demonstrated that it completed and publicly posted all required PIAs.
- The FISMA report for 2021 contained a recommendation to perform a feasibility analysis on applying document labeling requirements to FDIC documents created prior to September 2020, the date of FDIC Directive 1350.04, *Document Labeling*. In 2022, the FDIC determined that applying requirements to legacy documents would not be feasible due to the estimated cost, person-hours, risks, and impacts.
- The FISMA report for 2019 noted that the FDIC had not fully implemented planned controls to protect sensitive information stored in hardcopy or in shared folders on its network. In 2022, the FDIC demonstrated that it was performing physical walkthroughs of its buildings and scanning its network shared folders for possible exposure of sensitive information.
- In December 2019, the OIG completed an audit that assessed the effectiveness of the FDIC's Privacy Program and issued 14 recommendations regarding privacy governance, documentation, and operations in accordance with OMB Circular A-130. As of July 2022, the recommendations were closed.

Nevertheless, we found that the FDIC had not fully implemented a process to label data, which would improve the effectiveness of automated controls in the protection of sensitive information, including PII.

[21] FDIC OIG Memorandum, *Background Investigations for Privileged Account Holders*, June 2022 https://www.fdicoig.gov/sites/default/files/publications/AEC-Memorandum-22-002.pdf

The FDIC Has Not Implemented Its Document Labeling Guide

In late 2016, the FDIC initiated its Data Protection Program (DPP) in order to provide the FDIC with standards, policies, support, and methods to identify, categorize, label, and protect PII and sensitive information. This effort included the creation of FDIC Directive 1350.04, *Document Labeling*, in September 2020 and the Document Labeling Guide in March 2021. Those documents established requirements for categorizing and labeling documents so that FDIC personnel can identify the sensitivity of the documents and apply protective measures as appropriate.

Implementation of Document Labeling is critical for the effective operation of the Data Loss Prevention tool. The DLP tool mitigates the risk of exfiltration by scanning outgoing data for keywords that are correlated with sensitive information. Divisions also provide input on sensitive format and content patterns to assist in developing DLP rules. However, the DLP tool's ability to perform assessments of sensitive information is limited without a standardized labeling program.

By 2021, the FDIC had begun piloting its labeling program to collect feedback. During this phase, the FDIC encouraged but did not mandate labeling. In our FISMA report for 2021, we issued a recommendation to implement the document labeling guide requirements across the organization. However, the FDIC does not anticipate full implementation for several months. Therefore, the FDIC cannot assess its own document labeling controls, and we could not evaluate whether the FDIC had implemented proper controls on a consistent basis.

Security Training

The *Security Training* Domain includes controls that address an agency's maturity in providing appropriate security awareness training to its personnel, contractors, and other system users. FISMA also requires agencies to report on the resources, including budget, staffing, and training, necessary to implement an agency security program.

During 2022, the FDIC's CIOO had conducted an assessment of the knowledge, skills, and abilities of its workforce. This assessment enabled the CIOO to identify training needs that can be aligned to support the FDIC's ongoing operations and IT modernization efforts. The FDIC also completed corrective actions for the following audit recommendation:

- In August 2021, the FDIC OIG noted in its report on Mobile Device Security and Management[22] that the FDIC's annual security training contained limited information on threats to mobile devices and security practices for mitigating those threats. In response, the FDIC updated its security training to address mobile device risks. The OIG closed this recommendation.

The FDIC OIG identified other issues in this Domain in its report addressing Critical Building Services,[23] related to contractors and subcontractors who did not complete required Information Security and

[22] FDIC OIG Report, *Security and Management of Mobile Devices*, AUD-21-004, August 2021, https://www.fdicoig.gov/sites/default/files/publications/AUD-21-004.pdf.
[23] FDIC OIG Report, *Security of Critical Building Services at FDIC owned Facilities*, AUD-21-003, March 2021, fdicoig.gov/sites/default/files/publications/AUD_21_003_Redacted.pdf

Privacy Awareness Training and Insider Threat and Counterintelligence Awareness Training. The OIG recommended that the FDIC include a provision in its future contracts requiring contractor and subcontractor personnel to complete requisite training. As of July 20, 2022, the FDIC's ORMIC was performing an internal review of the actions taken to address the recommendation. Therefore, this recommendation remains unimplemented.

DETECT

The objective of the *Detect* Function is to implement continuous monitoring of control activities to discover and identify cybersecurity events in a timely manner. Cybersecurity events[24] include anomalies and changes in the organization's IT environment that may impact organizational operations, including mission, capabilities, or reputation.

Information Security Continuous Monitoring

NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (September 2011), defines an organization-wide approach to continuous monitoring that supports risk-based decision making at the organization, mission/business process, and information systems tiers.

The FDIC established and implemented policies and guidance to support the continuous monitoring of its information systems.[25] The FDIC followed the steps from the NIST RMF to authorize information systems with an authorization to operate (ATO)[26] decision letter before placing systems into production. The FDIC also assessed information system controls to determine if they are implemented correctly, operating as intended, and producing the desired outcome.

The FDIC completed corrective actions for an audit recommendation issued in our FISMA report for 2020 related to ensuring that cloud systems are subject to security and privacy control assessments (SCAs). Specifically, the FDIC performed annual control assessments in accordance with its Security Control Assessment Methodology for the 14 cloud systems that we identified as not being subject to annual SCAs. The OIG closed this recommendation.

Nevertheless, the FDIC did not consistently authorize all of its systems and subsystems with the NIST RMF as prescribed by OMB policy.

The FDIC Did Not Adequately Oversee and Monitor its Information Systems

FISMA requires Federal agencies to implement an information security program that provides security for the information and information systems that support the operations and assets of the agency,

[24] https://csrc.nist.gov/glossary/term/cybersecurity_event

[25] FDIC Directive 1310.3, *Information Security Risk Management Program* (March 2020), and the *Information Security Continuous Monitoring (ISCM) Strategy* (May 2022).

[26] The ATO is an official management decision by a senior Federal official, or Authorizing Official, to approve operation of an information system and to explicitly accept the risk to agency operations, assets, data, individuals, other organizations, and the Nation based on the implementation of a set of security and privacy controls.

including those provided or managed by contractors and other entities. These requirements apply to both systems that are owned and operated by the agency and systems that are outsourced to external vendors. According to NIST, outsourced information systems and services pose unique security risks, because they are not always developed or operated by agency personnel or at agency facilities, and may not benefit from the common security controls that typically protect the agency's information systems and data. FISMA and OMB policy require agencies to ensure that vendors handling sensitive information and operating systems on behalf of the Federal Government meet the same security and privacy requirements as Federal agencies.

The FDIC had previously subjected outsourced systems to an internally developed authorization and assessment methodology called the *Outsourced Solution Assessment Methodology* (OSAM). However, during 2020, the FDIC CIOO rescinded the OSAM. According to the CISO, the approach defined in OSAM for conducting security assessments of outsourced providers did not align with the RMF [27] defined in NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations* (December 2018). As a result, we concluded that the FDIC had not conducted proper security risk assessments over these systems, nor ATOs, or ongoing monitoring as required by the RMF. OMB Circular A-130 requires Federal agencies to follow the RMF. The OIG identified the oversight and monitoring of outsourced systems as a weakness for the FDIC in its Top Management and Performance Challenges for 2020 and 2021.[28]

In 2021, the FDIC OCISO acknowledged that many of its operational systems and subsystems were not subject to the RMF. Although many of the systems and subsystems were authorized under legacy methodologies, many of them did not comply with RMF requirements (see **Appendix IV** for the system list). To remediate this finding, the FDIC OCISO developed a "Legacy Approval Action Plan" whereby it would conduct RMF authorizations for systems and subsystems under legacy authorizations and subject them to RMF continuous monitoring requirements thereafter. This Plan includes conducting a review of the FDIC's current systems inventory and outsourced services covered by legacy authorization methods to ensure that all systems and subsystems are properly categorized and subject to the RMF. As of May 2022, the FDIC CIOO had completed the authorization for 73 of the 151 legacy systems and subsystems (approximately 48 percent), and it intends to complete the remaining 78 systems (52 percent) by March 2023.

If the FDIC does not consistently subject its systems to the RMF as we recommended in our FISMA report for 2021, it cannot ensure that security and privacy risks associated with these systems will be identified and addressed in a timely manner. The lack of adequate security oversight and monitoring of outsourced systems means that the FDIC will have less assurance that its systems are compliant with its security requirements, placing the confidentiality, integrity, and availability of these systems and the data they process at risk. Further, the FDIC may not have the necessary information to make efficient and effective risk management decisions about these systems supporting its mission and business functions.

---

[27] According to NIST SP 800-37, Rev. 2, the RMF consists of (1) preparing to execute the RMF by establishing context and priorities for managing security and privacy risks, (2) categorizing systems and data based on risk, (3) selecting and tailoring controls, (4) implementing controls, (5) assessing control effectiveness, (6) authorizing systems to operate, and (7) monitoring systems and controls on an ongoing basis.

[28] FDIC OIG Report, *Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation,* February 2021, https://www.fdicoig.gov/sites/default/files/attachments/TMPC-Final-18Feb21.pdf; and FDIC OIG Report, *Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation,* February 2022 https://www.fdicoig.gov/sites/default/files/attachments/TMPC_FINAL_Feb22.pdf

RESPOND

The objective of the *Respond* Function is to implement processes to contain the impact of detected cybersecurity events. Such processes include developing and implementing incident response plans and procedures, analyzing security events, and effectively communicating incident response activities.

Incident Response

FISMA requires each agency to develop, document, and implement an agency-wide information security program that includes policies and procedures for incident response.

The FDIC had established policies and procedures for responding to computer security incidents;[29] issued an updated agency-wide Incident Response Plan; operated a centralized system to track and manage incidents; and implemented a Computer Security Incident Response Team (CSIRT). These controls were consistent with incident response practices described in NIST SP 800-61, Rev. 2. The FDIC had implemented its incident response plan, policy, and procedures to classify and report incidents consistent with the Attack Vectors Taxonomy[30] defined by the United States Computer Emergency Readiness Team (US-CERT).

RECOVER

The objective of the *Recover* Function is to develop and implement activities to maintain plans for resilience and to restore capabilities or services impaired due to a cybersecurity incident. The *Recover* Function supports the timely recovery of normal operations to reduce the impact of a cybersecurity incident, including recovery planning, improvements, and communications.

Contingency Planning

FISMA requires agencies to develop, document, and implement plans and procedures to ensure the continuity of operations for information systems that support the operations and assets of the organization. The FDIC had performed Business Impact Analyses to calculate the system criticality for our two systems used by the FDIC – FDICconnect (FCX) and Enterprise Data Management General Support System (EDM GSS) (see description of the two systems in **Appendix I**). In addition, in October 2021 the FDIC performed a contingency plan test by failing over and failing back[31] mission-critical and mission-essential applications to and from the Backup Data Center. The test included complicating factors, such as removing key personnel during the exercise without notice, to simulate difficulties in a real disaster event. The test was performed in a remote environment resulting from the telework requirements. The FDIC developed a comprehensive After Action Report (AAR) that described the overall success of the Disaster Recovery Team in achieving its objectives as well as the lessons learned.

---

[29] FDIC Directive 1360.12, *Reporting Information Security Incidents* (April 2017), and *Security Response Team (SRT) Event Management Standard Operating Procedure (SOP)* (September 2021).
[30] The US-CERT established a standard taxonomy of potential attack sources to assist incident communication efforts throughout the federal government. Attack sources include email, impersonation, and improper usage.
[31] A failover operation is the process of switching production to a backup location. Failback is the process of returning production to its original location.

The AAR noted that although all 48 tested applications failed over and back within the required time period, two systems experienced connectivity issues and one system experienced data loss in the backup environment. The AAR included 38 follow-up actions designed to improve documentation requirements, identify personnel needs, enhance communication between test personnel, and troubleshoot technical concerns identified during the test.

CONCLUSION

The FDIC established a number of controls and practices consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines. Our report contains one recommendation and cites three unimplemented recommendations from FISMA reports in prior years, as noted in Appendix II, other unimplemented OIG recommendations, and the FDIC's POA&Ms and information security initiatives. These recommendations and initiatives aim to strengthen the effectiveness of the FDIC's information security program controls and practices.

APPENDIX I – SCOPE AND METHODOLOGY

Cotton conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (2018 revision). These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We assessed internal controls that we deemed significant to the audit objective. Specifically, we assessed five components of internal control, and 11 associated principles as defined in the Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* (September 2014) (Green Book).[32] However, the scope of our assessment of internal controls was limited to the OMB Office of the Federal Chief Information Officer *Fiscal Year (FY) 2022 Core IG Metrics Implementation Analysis and Guidelines* (DHS FISMA Reporting Metrics), which we used to assess the effectiveness of the FDIC's information security program and practices. Accordingly, our work may not have identified all internal control deficiencies in the FDIC's information security program and practices that existed at the time of our audit.

To accomplish our objective, we:

- Evaluated key components of the FDIC's information security program plans, policies, procedures, and practices that were in place as of June 1, 2022 (or as otherwise noted in our report) for consistency with FISMA, NIST security standards and guidelines, and OMB policies and guidance. We considered guidance contained in OMB's Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements* (December 2021), when planning and conducting our work.
- Assessed the maturity of the FDIC's information security program with respect to the metrics defined in the DHS FISMA Reporting Metrics. As discussed above, the DHS FISMA Reporting Metrics provide a framework for assessing the effectiveness of agency information security programs.
- Considered the results of recent and ongoing audit and evaluation work, conducted by the FDIC OIG and the GAO, relating to the FDIC's information security program controls and practices.
- Selected and evaluated security controls related to a non-statistical sample of two FDIC-maintained information systems, *FDICconnect* and *Enterprise Database Management*. Our analysis of these systems included reviewing selected system documentation and other relevant information, as well as testing selected security controls. The systems are described below:

    - *FDICconnect (FCX)*
      FCX is a web-based application used to transact business with insured financial institutions, authorized non-banking entities, and state banking department examiners. Banks use a number of business transactions hosted under FCX to submit and retrieve information from FDIC business systems. FCX performs user authentication, displays a menu of transaction

[32] The Green Book organizes internal control through a hierarchical structure of 5 components and 17 principles. The 5 components consist of the Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring. The 17 principles support the effective design, implementation, and operation of the components, and represent the requirements that are necessary to establish an effective internal control system.

options, and mediates secure communication through a firewall. Authorized FDIC personnel use administrative transactions to manage the FCX environment and produce system reports.

- *Enterprise Data Management (EDM) General Support System (GSS)*
  The EDM GSS is comprised of the FDIC's relational database management systems, which include (b) (7)(E) . These systems serve as the primary backend databases to many of the FDIC's on-premises applications and mission-essential systems, including FCX.

We selected the systems described above because they contain large quantities of sensitive information and/or support mission-essential functions.[33] A disruption of FCX and/or EDM could impair the FDIC's business transactions and services necessary for operations, ultimately hindering the FDIC's ability to achieve its mission.

Cotton conducted the audit remotely at its off-site location in the Washington, D.C. metropolitan area from March through July 2022.

[33] According to FDIC Directive 1360.13, *IT Continuity Implementation Program*, a Mission Essential Function (MEF) is directly related to accomplishing an organization's mission as set forth in its statutory or executive charter. Any IT application, system, or service that supports a MEF is deemed "mission essential" and is designated a recovery time of 0-12 hours.

APPENDIX II – STATUS OF PRIOR-YEAR FISMA RECOMMENDATIONS

The following table summarizes our determinations regarding the status of previously unaddressed recommendations from FISMA audit reports issued in 2016, 2019, 2020, and 2021. Recommendations marked 'Closed' denote Status updates that followed the publication of the FISMA report in 2021.

Recommendation	Status
Report Issued in 2016, Recommendation 5 Review existing resource commitments and priorities for addressing the Data Communications (DCOM) Plan of Actions and Milestones (POA&Ms) and take appropriate steps to ensure they are addressed in a timely manner.	Closed
Report Issued in 2019, Recommendation 2 Monitor employee and contractor compliance with policy requirements for properly safeguarding sensitive electronic and hardcopy information.	Closed
Report Issued in 2020, Recommendation 3 Remediate incomplete and out-of-date baseline configurations.	Closed
Report Issued in 2020, Recommendation 4 Assess the effectiveness of the FDIC's controls for managing Administrative Accounts and implement control improvements.	Closed
Report Issued in 2020, Recommendation 5 Implement a process to ensure that all outsourced information systems are subject to the NIST Risk Management Framework as prescribed by OMB policy.	Closed
Report Issued in 2020, Recommendation 6 Ensure that the FDIC's cloud-based information systems are subject to annual security and privacy control assessments.	Closed
Report Issued in 2021, Recommendation 1 Develop and implement SCRM processes and procedures in accordance with the Supply Chain Risk Management Program Directive and applicable government guidance.	Unimplemented
Report Issued in 2021, Recommendation 2 Begin tracking completion of ICAM milestones of its revised ICAM Roadmap.	Closed
Report Issued in 2021, Recommendation 3 Complete implementation of the PCM process to include updating PIAs for all required systems.	Closed
Report Issued in 2021, Recommendation 4 Implement Document Labeling Guide requirements across the entire organization as dictated by business needs.	Unimplemented
Report Issued in 2021, Recommendation 5 Perform an analysis of the feasibility of applying the Document Labeling Guide for documents that were created before the issuance of the directive.	Closed
Report Issued in 2021, Recommendation 6 Ensure that the FDIC's in-house and contractor-managed information systems are subject to a formal authorization process as defined in the Risk Management Framework.	Unimplemented

APPENDIX III – LIST OF ACRONYMS

Acronym	Description
AAR	After Action Report
AD	Active Directory
AIS	Automated Information System
APS	Automated Procurement System
ARCS	Access Request and Certification System
ATO	Authorization to Operate
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CINO	Chief Innovation Officer
CIO	Chief Information Officer
CIOO	Chief Information Officer Organization
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CISR	Division of Complex Institution Supervision and Resolution
CPO	Chief Privacy Officer
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerability and Exposure
DCOM	Data Communications
DCP	Division of Depositor and Consumer Protection
DHS	Department of Homeland Security
DIR	Division of Insurance and Research
DIT	Division of Information Technology
DLP	Data Loss Prevention
DOA	Division of Administration
DOD	Department of Defense
DOF	Division of Finance
DPP	Data Protection Program
DRR	Division of Resolutions and Receiverships
EDM GSS	Enterprise Data Management General Support System
EDR	Endpoint Detection and Response
EO	Executive Order
FCX	FDICconnect
FDIC	Federal Deposit Insurance Corporation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAO	Government Accountability Office
GSS	General Support System
ICAM	Identity, Credential, and Access Management

IG	Inspector General
ISCM	Information Security Continuous Monitoring
ISM	Information Security Manager
ISSM	Information Systems Security Manager
IT	Information Technology
ITRAC	IT Risk Advisory Council
Legal	Legal Division
MEF	Mission Essential Function
NCP	National Checklist Program
NIST	National Institute of Standards and Technology
OCISO	Office of the Chief Information Security Officer
OCOM	Office of Communications
OIG	Office of Inspector General
OMB	Office of Management and Budget
ORMIC	Office of Risk Management and Internal Controls
OSAM	Outsourced Solution Assessment Methodology
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Actions and Milestones
RBAC	Role-Based Access Control
RMF	Risk Management Framework
RMS	Division of Risk Management Supervision
SAOP	Senior Agency Official for Privacy
SCA	Security Control Assessment
SCRM	Supply Chain Risk Management
SI-2	Flaw Remediation, a NIST SP-800 53. Rev 5 control
SOP	Standard Operating Procedure
SP	Special Publication
SRT	Security Response Team
US-CERT	United States Computer Emergency Readiness Team

(b) (7)(E)

(b) (7)(E)

Part II

****

FDIC Comments and OIG Evaluation

FDIC Comments and OIG Evaluation

The FDIC's Chief Information Officer (CIO) and Chief Information Security Officer (CISO) provided a written response, dated September 20, 2022, to a draft of the report. The response is presented in its entirety beginning on page II-2. In the response, the CIO and CISO concurred with the report's recommendation. The recommendation will remain open until we confirm that corrective actions have been completed and are responsive. A summary of the FDIC's corrective actions begins on page II-5

CONTROLLED//FDIC BUSINESS

FDIC
3501 Fairfax Drive, Arlington, VA 22226-3500
Chief Information Officer & Chief Privacy Officer

September 20, 2022

TO: Terry L. Gibson
Assistant Inspector General for Audits, Evaluations, and Cyber

FROM: Sylvia W. Burns
Chief Information Officer and Chief Privacy Officer
SYLVIA BURNS Digitally signed by SYLVIA BURNS Date: 2022.09.20 12:18:35 -04'00'

Zachary N. Brown
Chief Information Security Officer
ZACHARY BROWN Digitally signed by ZACHARY BROWN Date: 2022.09.20 11:26:04 -04'00'

SUBJECT: Management Response to the Draft Audit Report Entitled, *The FDIC's Information Security Program–2022* (No. 2022-006)

Thank you for the opportunity to review and comment on the subject draft audit report issued by the Office of Inspector General (OIG) on September 1, 2022. The report details the results of the OIG's audit of the Federal Deposit Insurance Corporation's (FDIC) information security program pursuant to the Federal Information Security Modernization Act of 2014 (FISMA). The OIG engaged Cotton & Company Assurance and Advisory, LLC to perform the audit. The effective implementation of the FDIC's information security program is critically important to the success of the agency's mission of maintaining stability and public confidence in the nation's financial system. Accordingly, information security is a top priority for the FDIC.

We are pleased that the audit determined that the FDIC's information security program is operating at a Level 4, "Managed and Measurable." In the context of the maturity model used by federal Inspectors General, a Level 4 signifies that the FDIC's information security program is operating at an effective level of security. We also appreciate the report's recognition of improvements made to the FDIC's information security program during the past year. Such improvements include the prioritization of remediation activities to address Plans of Action and Milestones (POA&Ms); improved safeguards for protecting sensitive information stored in hardcopy and electronic format; updated security training to address risks associated with mobile devices; and enhanced privacy controls. Additional improvements have been made since the close of the audit. For example, we upgraded our legacy system authorizations to align with the National Institute of Standards and Technology's Risk Management Framework (RMF) for more than 70 percent of the FDIC's information systems. This figure is up from approximately 50 percent as of the time of the audit. We expect to address authorizations for the remaining systems by March 2023. Further, the audit report noted that the FDIC closed 9 recommendations made during the OIG's prior-year FISMA audits.

The audit report also identifies areas for improvement, including the continued maturation of our supply chain risk management program and in the areas of systems oversight and monitoring, POA&Ms, privileged account management, and document labeling. The FDIC will continue to place priority attention on these areas.

FDIC

3501 Fairfax Drive, Arlington, VA 22226-3500 Chief Information Officer & Chief Privacy Officer

Although not addressed in the audit report, the OIG's Executive Summary references personnel changes over the past year, including the resignations of the FDIC's Chief Innovation Officer and Chief Data Officer (CDO). Both positions have been filled with permanent individuals. Notably, the prior CDO provided the FDIC almost a year of advance notice before departing. This allowed the FDIC to hire a new CDO to work alongside the incumbent for more than 2 months to ensure a smooth transition. The OIG's Executive Summary also references the organizational realignment of FDITECH into the Chief Information Officer Organization (CIOO) in July 2022 and the establishment of two new Deputy CIOs. This realignment allows the FDIC to build upon the successful partnership between FDITECH and CIOO and facilitates the implementation of new technologies and ideas at the FDIC. It also furthers ongoing efforts to modernize the FDIC's internal IT operations.

[redacted]

The OIG's Executive Summary adds that the FDIC made changes to its IT infrastructure, including the accelerated adoption of cloud services. The flexibility and scalability of cloud allowed the FDIC to meet the urgent challenges of the pandemic, such as large surges in demand for services and the sudden shift to remote work. These changes also strengthened our security posture and improved the availability of IT resources.

The OIG's Executive Summary discusses another matter not referenced in the audit report. Specifically, FDIC employees and/or contractors perform manual reviews of emails flagged by automated tools, and this process presents potential security and privacy risks because reviewers can be inadvertently exposed to information they would otherwise not be permitted to view. The OIG noted that this process also presents risk that emails relevant to urgent law enforcement matters are not received by the OIG in a timely manner, thus presenting security and safety concerns. The CIOO has implemented a multi-layered set of controls to protect the FDIC's network, systems, and data from security risks associated with email. The CIOO has also taken steps to help ensure the confidentiality and timely delivery of email to the OIG, and leadership and staff in the CIOO and OIG continue to meet on a regular basis to discuss this matter and potential improvements.

The audit report contains one recommendation addressed to the CIO. The FDIC concurs with this recommendation and is committed to addressing it as part of its continuing efforts to maintain an effective information security program.

CONTROLLED//FDIC BUSINESS

FDIC
3501 Fairfax Drive, Arlington, VA 22226-3500
Chief Information Officer & Chief Privacy Officer

MANAGEMENT RESPONSE

Recommendation 1 –

We recommend that the CIO:

1. Address the 31 POA&Ms identified as of June 21, 2022, associated with NIST SP 800-53 Rev. 5 control SI-2 (Flaw Remediation).

   Management Decision: Concur

   Corrective Action: The CIOO will address the identified 31 POA&Ms.

   Estimated Completion Date: 3/31/2023

If you have any questions regarding this response, please contact Akemi Burdick, Acting Chief, Policy, Audits, Compliance, and Risk Section, at akeburdick@FDIC.gov.

cc: E. Marshall Gentry, Chief Risk Officer and Director, Office of Risk Management and Internal Controls
Gregory S. Kempic, Office of Risk Management and Internal Controls
Mark F. Mulholland, Deputy Chief Information Officer for Management

Summary of the FDIC's Corrective Actions

This table presents management's response to the recommendations in the report and the status of the recommendations as of the date of report issuance.

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	The CIOO will address the identified 31 POA&Ms.	March 31, 2023	$0	Yes	Open

[a] Recommendations are resolved when —

1. Management concurs with the recommendation, and the planned, ongoing, and completed corrective action is consistent with the recommendation.
2. Management does not concur with the recommendation, but alternative action meets the intent of the recommendation.
3. Management agrees to the OIG monetary benefits, or a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b] Recommendations will be closed when the OIG confirms that corrective actions have been completed and are responsive.

Federal Deposit Insurance Corporation
Office of Inspector General

3501 Fairfax Drive
Room VS-E-9068
Arlington, VA 22226

(703) 562-2035

******

The OIG's mission is to prevent, deter, and detect waste, fraud, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the agency.

To report allegations of waste, fraud, abuse, or misconduct regarding FDIC programs, employees, contractors, or contracts, please contact us via our Hotline or call 1-800-964-FDIC.