Office of Inspector General

The Federal Deposit Insurance Corporation's Information Security Program – 2023

September 2023 **No. AUD-23-004**

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

OIG

Office of Inspector General

NOTICE

Pursuant to Pub. L. 117-263, section 5274, non-governmental organizations and business entities identified in this report have the opportunity to submit a written response for the purpose of clarifying or providing additional context to any specific reference. Comments must be submitted to comments@fdicoig.gov within 30 days of the report publication date as reflected on our public website. Any comments will be appended to this report and posted on our public website. We request that submissions be Section 508 compliant and free from any proprietary or otherwise sensitive information.

Executive Summary

The FDIC's Information Security Program–2023

The Federal Information Security Modernization Act of 2014 (FISMA), Public Law No. 113-283, requires Federal agencies, including the Federal Deposit Insurance Corporation (FDIC or Corporation), 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) 2023 – 2024 Inspector General FISMA Reporting Metrics* (Department of Homeland Security [DHS] FISMA Reporting Metrics).

To support compliance with FISMA, the DHS FISMA Reporting Metrics provide a methodology for 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 2021, DHS, OMB, and the Cybersecurity and Infrastructure Security Agency (CISA) published a total of 66 Metrics, 57 of which related to specific controls and 9 summary metrics allowing IGs to provide additional information for each Domain. In FY 2022, IGs were required to evaluate a subset of 20 "Core" FISMA metrics, which represented a combination of OMB priorities and other critical controls. The remaining 37 Metrics were classified as "Supplemental," which will be reviewed every other year on an alternating basis. In FY 2023, IGs were required to evaluate the 20 Core metrics in addition to 20 of the remaining 37 Supplemental metrics.

OMB and the Council of the Inspectors General on Integrity and Efficiency adjusted the FISMA scoring system for FY 2023. IGs are 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. Prior to FY 2023, the most common or frequently occurring Metric rating (mode) was used as the basis for calculating the organization's overall maturity rating. In FY 2023, the scoring mechanism changed to require the use of calculated averages, which are computed by adding a set of numbers and then dividing by the count of those numbers. Additionally, the DHS FISMA Reporting Metrics recommended that IGs use the calculated averages of the Core metrics and Supplemental metrics as data points when determining an overall maturity rating for the organization.

For FY 2023, the overall organizational information security program maturity level was determined using the calculated average method of the (1) Core metric average rating and (2) Supplemental metric average rating. These two ratings were used alongside a subjective analysis of identified control weaknesses to determine an overall program-level rating. Regardless of the calculation method used, a single number would not fully capture the nature, scope, and magnitude of the risk posture of an agency's information security program.

Results

Cotton determined that the FDIC's overall information security program was operating at a Maturity Level 4 (Managed and Measurable) with respect to the FY 2023 FISMA Metrics. In reaching this determination, Cotton's assessment was aligned with the methodology and scope required by the DHS FISMA Reporting Metrics. We caution the FDIC against complacency since deficiencies remain in the information security program at the FDIC.

Cotton 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 NIST security standards and guidelines. In addition, the FDIC completed certain actions to continue to strengthen its security controls since last year (e.g., fully implementing Document Labeling requirements across the organization and completing Risk Management Framework (RMF) authorizations for all applications originally authorized under legacy system authorization methodologies).

However, Cotton found security control weaknesses that reduced the effectiveness of the FDIC's information security program and practices that could be improved to reduce the effect on the confidentiality, integrity, and availability of the FDIC's information systems and data. In many cases, these security control weaknesses were identified during ongoing or completed OIG audits and evaluations, or through FDIC security and privacy control assessments. 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 Needs to Fully Implement a Software Inventory Automation Program to Manage End-of-Life and End-of-Service Assets:** We found that the FDIC's platform for monitoring software assets contained unreliable data that limited the FDIC's ability to manage software approaching or reached end-of-life or end-of-service.
- **The FDIC's Supply Chain Risk Management (SCRM) Program Lacks Maturity:** The FDIC is still developing policies and procedures to address the SCRM finding from the FY 2021 FISMA report. Additionally, the OIG evaluation report of The FDIC's Implementation of Supply Chain Risk Management (issued March 2022) noted that the FDIC did not implement several objectives outlined in its SCRM Implementation Project Charter, did not conduct supply chain risk assessments in accordance with best practices, did not ensure that its Enterprise Risk Management processes fully capture supply chain risks, and FDIC Contracting Officers did not maintain contract documents in the proper system. The OIG issued nine recommendations, five of which remain unimplemented as of July 28, 2023.
- **The FDIC Did Not Remove Accounts Belonging to Separated Personnel in a Timely Manner:** The FDIC did not consistently remove accounts for individuals who departed the FDIC. Of the accounts belonging to 44 employees and contractors sampled that departed the FDIC in 2023, six accounts belonging to three employees and two contractors were not disabled within one business day of the user separation as required. Access for the six accounts was removed between 4 and 84 days after the user separation date, including one privileged account.
- **The FDIC Did Not Configure Privileged Accounts in Accordance with Principle of "Least Privilege":** In the audit report of the FDIC's Security Controls Over Windows Active Directory (issued March 2023), the OIG identified several instances where accounts were configured with elevated account settings that were not needed for administrators to perform their business roles, as well as other instances where users had elevated access longer than needed. The OIG issued 15 recommendations, five of which directly related to privileged accounts and remain unimplemented as of July 28, 2023.

- **The FDIC Needs to Enforce Cybersecurity and Privacy Awareness Training Requirements**: We found that over 400 personnel did not complete Cybersecurity and Privacy Awareness Training as required. Employees and contractors are required to complete security and privacy training within 5 business days of receiving network equipment and annually thereafter. Failure to comply with mandatory security and privacy training may lead to user access being revoked. As of July 13, 2023 (13 days after the training due date), these users retained access to FDIC network and resources despite not having completed the required training due to technological issues that arose upon restricting user access.

Recommendations

The FISMA audit report contains two new recommendations related to weaknesses identified during this year's audit. The FDIC concurred with the recommendations and plans to complete corrective actions by June 28, 2024. Additionally, **Appendix II** contains a listing of the two unimplemented recommendations from prior FISMA reports, on which the FDIC should focus attention. These recommendations aim to strengthen the effectiveness of the FDIC's information security program controls and practices.

Contents

Part I

Report by Cotton & Company Assurance and Advisory, LLC
The FDIC's Information Security Program – 2023 **I-1**

Part II

FDIC Comments and OIG Evaluation **II-1**

FDIC Comments **II-2**

Summary of the FDIC's Corrective Actions **II-4**

Part I

****

Report by Cotton & Company Assurance and Advisory, LLC

THE FEDERAL DEPOSIT INSURANCE CORPORATION'S INFORMATION SECURITY PROGRAM – 2023

AUDIT REPORT

SEPTEMBER 25, 2023

Cotton

A SIKICH. COMPANY

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

TABLE OF CONTENTS

Introduction 5
Audit Objective 6
DHS FISMA Reporting Metrics and the NIST Cybersecurity Framework 6
Overview of the FDIC's Information Security Program 12
Summary of Results 13
Audit Results 15
Identify 15
Risk Management 15
Supply Chain Risk Management 17
Protect 18
Configuration Management 18
Identity and Access Management 19
Data Protection and Privacy 21
Security Training 22
Detect 23
Information Security Continuous Monitoring 23
Respond 24
Incident Response 24
Recover 25
Contingency Planning 25
Conclusion 26
Appendix I – Objective, Scope, and Methodology 27
Appendix II – Status of Prior-Year FISMA Recommendations 29
Appendix III – List of Acronyms 30

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 – 2023

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 February through July 2023.

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)

Simon Lee, CISA, CISSP
Director

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. According to the National Vulnerability Database, the publicly accessible U.S. government repository of vulnerability data, 2,395 vulnerabilities were identified in June 2023 alone. According to an analysis by CISA, of the over 160,000 vulnerabilities in the National Institute of Standards and Technology (NIST) National Vulnerability Database released by November 2021, 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 in the database).[1]

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 Personally Identifiable Information (PII) and sensitive business information, including 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, that FDIC 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)[2] 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.

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:

[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] Pub. L. No. 113-283, 128 Stat. 3073 (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.

- 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),[3] 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 plays a lead role in strengthening 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) 2023-2024 IG FISMA Act of 2014 Reporting Metrics* (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 high level. Aligning the DHS FISMA Reporting Metrics with the NIST Cybersecurity Framework ensures that IGs 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

[3] 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.

consistency among IG FISMA evaluations. The DHS FISMA Reporting Metrics divide the five function areas into nine Domains, which are high-impact control families that correspond to the objectives of the function areas. 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**

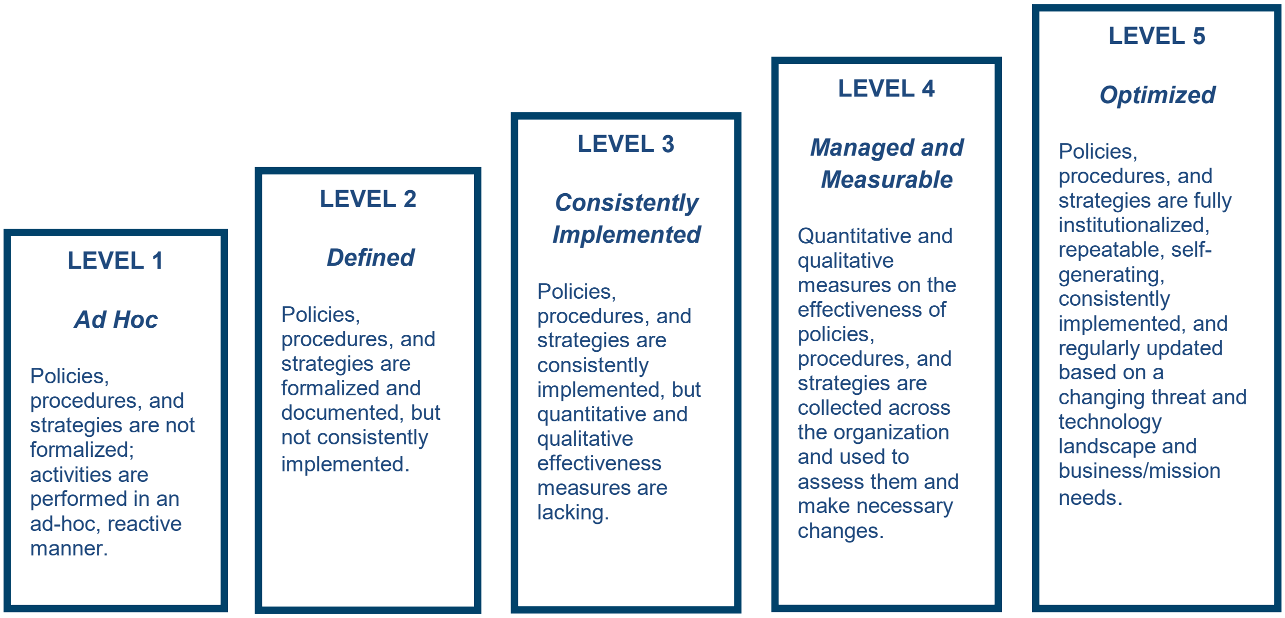
Source: Cotton's analysis of the NIST Cybersecurity Framework and DHS FISMA Reporting Metrics.

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*) or higher indicates that the information security program is operating at an effective level of security.[4]

[4] Information regarding the determination of maturity level ratings can be found at https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act.

Figure 1: FISMA Maturity Model Levels



LEVEL 1

Ad Hoc

Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.

LEVEL 2

Defined

Policies, procedures, and strategies are formalized and documented, but not consistently implemented.

LEVEL 3

Consistently Implemented

Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.

LEVEL 4

Managed and Measurable

Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.

LEVEL 5

Optimized

Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: DHS FISMA Reporting Metrics.

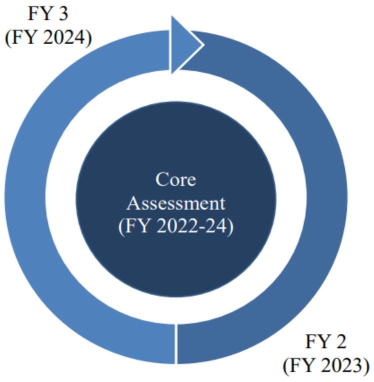
The DHS FISMA Reporting Metrics encourage IGs to consider a holistic, risk-based approach for determining the overall rating of an organization's information security program. However, it highlights the use of a non-weighted, calculated average rating methodology, which contrasts with the previous mode-based scoring system. The following section, "Changes to DHS FISMA Reporting Metrics" provides additional details on the scoring change.

Changes to DHS FISMA Reporting Metrics

In FY 2021, IGs were required to assess 66 metrics annually and submit their results at the end of October. As shown in Figure 2, in FY 2022, OMB and CIGIE introduced substantial changes as they shifted the evaluation process to a multi-year cycle beginning in FY 2022. Specifically:

- IGs are 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 are the "Core" Metrics.
- The remaining metrics are divided in two groups, each to be evaluated every other year. These are collectively the "Supplemental" Metrics.
- In FY 2023, IGs will test the 20 Core Metrics and 20 Supplemental Metrics.
- 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 to better allow each agency to request funding to remediate findings in a timely manner.

Figure 2: FISMA Assessment Schedule



Source: OMB Memo M-22-05

OMB and CIGIE also adjusted the FISMA scoring system. Prior to FY 2023, IGs were instructed to use the most common rating (mode) across Domains and Function Areas to calculate the overall information security program rating. The FY 2023 DHS FISMA Reporting Metrics introduce a calculated average approach, wherein the numerical average of the metrics in each Domain establishes the foundation of the overall information security program rating level. DHS encourages IGs to consider the results of this calculation among multiple data points when determining an overall rating. Suggested data points include the following:

- Results of Core Metrics, as those tie directly to Administration priorities and other high-risk areas;
- Calculated averages of Supplemental Metrics;
- The results of cybersecurity evaluations, including system security control reviews, vulnerability scanning, and penetration testing conducted during the review period;
- The progress made by agencies in address outstanding IG recommendations; and,
- Security incidents reported during the review period.

Changes to the scoring system potentially affect an organization's overall rating in relation to the rating last year. These changes, together with differences in the scope of Metric evaluations performed each year and changes within individual Metrics criteria or objectives, make it inadvisable to compare this year's maturity ratings to prior or future year ratings.

Zero Trust Architecture

OMB Memorandum 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*." M-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. Starting in FY 2022, OMB began mapping Zero Trust Architecture control activities to specific FISMA Metrics. For example, one Identify function area Metric evaluates the organization's adoption of authentication mechanisms, which is relevant to the Identity objective. The FY 2023 FISMA guidance listed in M-23-03 states OMB will continue to align performance management under FISMA with benchmarks for the implementation of Zero Trust Architecture.

In FY 2022, the FDIC developed and submitted a Zero Trust Implementation Plan to OMB in accordance with M-22-09 and assembled a Core Team and Task Force responsible for Implementation. During FY 2023, the FDIC expanded its Zero Trust Program, including developing a Zero Trust Charter that assigns individual task owners for each Zero Trust Task and performing a gap analysis based on a three-level maturity model. We determined that the FDIC currently complies with all M-22-09 requirements.

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.

We determined during the FY 2022 FISMA audit that the FDIC implemented an EDR solution and provided CISA with access to it. CISA did not identify any gaps in the FDIC's EDR solution concerning compliance with OMB Memorandum M-22-01 and EO 14028.

Supply Chain Risk Management

The FY 2021 DHS FISMA Reporting Metrics introduced the Supply Chain Risk Management (SCRM) Domain within the Identify Function. The SCRM Domain highlights the dependence on products, systems, and services from external providers, presenting additional risks to an organization. These risks include the insertion or use of counterfeits, tampering, insertion of malicious software and hardware, and poor manufacturing and development practices in the supply chain. The risks in the Federal Government's supply chain were acknowledged by the Federal Acquisition Supply Chain Security Act of 2018,[5] which directed agencies to assess, avoid, mitigate, accept, or transfer supply chain risks.

On September 14, 2022, OMB released Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Process*, which provides implementation guidance to Federal Agencies on how to ensure that their third-party software complies with NIST guidance for secure software development practices. The Memorandum requires agencies to inventory all software with a separate inventory for critical software. They must then develop a consistent process to communicate the necessary NIST secure software development Guidance with their software vendors. Agencies will then collect vendor self-attestations (or equivalent documentation) confirming that the vendor complies with the necessary software development practices. M-22-18 further directs CISA to develop a self-attestation form template to support the effort. In June 2023, OMB extended deadlines to obtain software attestations for critical and non-critical software until 3 and 6 months after it approves the template, respectively.

[5] The Federal Acquisition Supply Chain Act of 2018, Title II of the SECURE Technology Act, Pub. L. No. 115-390, 132 Stat. 5173.

As of July 28, 2023, the FDIC is operating at a Level 1 (Ad Hoc) maturity level for the SCRM Domain due to open recommendations related to the ongoing implementation of SCRM processes and procedures that are described in more detail below.

Event Logging

On August 27, 2021, OMB released Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*. The Memo highlighted system logs as a critical resource to detect, investigate, and remediate cyber threats. OMB also established standards for logged events, log retention, and log management, with a focus on ensuring centralized access and visibility for the enterprise security operations center (SOC) for each agency.

Appendix C of the Memorandum lists all the log categories that should be captured, ranging from highest (Criticality 0) to lower (Criticality 3) criticalities. The Memorandum also describes requirements for how logs are to be structured and managed, including a timestamp standard, log access, and protecting log information. Each agency and all of its components are measured for compliance with these requirements using four maturity levels, ranging from EL0 through EL3:

- EL0: Not Effective – Logging requirements of highest criticality are either not met or are only partially met.
- EL1: Basic – Only logging requirements of highest criticality are met.
- EL2: Intermediate – Logging requirements of highest and intermediate criticality are met.
- EL3: Advanced – Logging requirements at all criticality levels are met.

The Memorandum details timelines for when agencies must reach each maturity level. Specifically:

- Within one year of the date of this memorandum (August 27, 2022), reach EL1 maturity.
- Within 18 months of the date of this memorandum (February 27, 2023), achieve EL2 maturity.
- Within 2 years of the date of this memorandum (August 27, 2023), achieve EL3 maturity.

As of July 28, 2023, the FDIC reached level EL1 as it was able to demonstrate that it could log the required events as well as collect, maintain, and protect event logs. The FDIC achieved EL1 during fieldwork. However, FDIC system owners and security personnel were continuing their collaboration to meet logging requirements for all logs required to reach EL2. Additionally, the FDIC was awaiting CISA's publication of supplemental guidance necessary for Federal agencies to document a standardized log structure (schema), which is an EL2 requirement.

Asset Visibility

CISA is an agency within the Department of Homeland Security (DHS) that leads the Federal cybersecurity effort. It maintains the Continuous Diagnostics and Mitigation (CDM) Program, which provides cybersecurity tools, integration services, and dashboards with participating Agencies to improve Agencies' security postures. Among its services is "Asset Management," whereby it identifies the inventory of hardware, software, and system assets in an organization and provides continuous monitoring services, such as identifying potential vulnerabilities.

On January 26, 2022, OMB released Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*, which provides guidance for the FISMA review in FY 2023 and outlines key initiatives. Among them is a requirement that agencies report at least 80 percent of their Government-furnished equipment (GFE) through the CDM program by the end of FY 2023.

On October 3, 2022, CISA released BOD 23-01 – *Improving Asset Visibility and Vulnerability Detection on Federal Networks*, which provides a list of required agency actions to fulfill the M-23-03 requirement. The requirements include specific asset discovery and vulnerability enumeration actions by April 3, 2023. We determined that the FDIC complied with the BOD 23-01 requirements. Specifically, through its vulnerability management program, the FDIC:

- Performed automated asset discovery on at least a weekly basis.
- Performed vulnerability scans on discovered assets at least every 14 days.
- Ingested vulnerability data from CDM on a daily basis.
- Initiated vulnerability scans on an ad hoc basis.

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. 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)[6] 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.

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 and privacy professionals within the Office of the CISO (OCISO), which is part of the Chief Information Officer Organization (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

[6] *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).

responsible for facilitating information security activities for contractor systems utilized within their Office/Division.

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), OIG, 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, Division/Office ISMs) for integrating and managing NIST Risk Management Framework (RMF) tasks and activities for systems within their assigned portfolios.

This FISMA assessment took place during a period of considerable IT transformation. For example, the FDIC has undertaken significant IT modernization efforts to reduce on-premises infrastructure and migrate systems to the cloud. The OIG noted in its July 2023 report on The FDIC's Adoption of Cloud Computing Services[7] that in 2021, the FDIC began its accelerated transition to the cloud after the issuance of Executive Order 14028, *Improving the Nation's Cybersecurity*, which required agency heads to update plans to prioritize the use of cloud technology. The FDIC's 2025 Target State Architecture Plan emphasizes a foundational transformation in the FDIC's IT portfolio management, and identifies accelerating cloud adoption as one of four overarching themes. To achieve this theme, the FDIC's Enterprise Strategy Branch plans to embrace commercial Federal Risk and Authorization Management-authorized cloud services to securely increase the visibility, scalability, and flexibility of IT capabilities.

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 risk of cyberattacks or incidents including the unauthorized access, use, disclosure, disruption, modification, or destruction of information or systems. 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 for the core and supplemental metrics, respectively, 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. Under the new 3 year FISMA reporting cycle, the scope of the Metrics varies year-over-year. These changes, together with anticipated differences in the scope of audit work performed in subsequent years, make it inadvisable to compare this year's maturity level ratings to ratings in both prior and future years.

[7] FDIC OIG Report, *The FDIC's Adoption of Cloud Computing Services*, July 2023. https://www.fdicoig.gov/reports-publications/audits-and-evaluations/fdics-adoption-cloud-computing-services

Table 2: Core Metric Ratings by Function Area and the Overall Information Security Program

Function Area	Domain	Function Area Rating	Overall Rating
Identify	Risk Management	3.5	3.88
	Supply Chain Risk Management		
Protect	Configuration Management	3.875	
	Identity and Access Management		
	Data Protection and Privacy		
	Security Training		
Detect	ISCM	4.00	
Respond	Incident Response	3.50	
Recover	Contingency Planning	4.50	

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

Table 3: Supplemental Metric Ratings by Function Area and the Overall Information Security Program

Function Area	Domain	Function Area Rating	Overall Rating
Identify	Risk Management	3.20	3.98
	Supply Chain Risk Management		
Protect	Configuration Management	3.70	
	Identity and Access Management		
	Data Protection and Privacy		
	Security Training		
Detect	ISCM	4.00	
Respond	Incident Response	4.50	
Recover	Contingency Planning	4.50	

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

Based on the overall ratings of the core metrics (3.88) and supplemental metrics (3.98), we determined that the FDIC is operating at a Level 4 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. In response to the recommendations made in our FISMA audit report in September 2022, the FDIC also took action to strengthen related security controls. For example, the FDIC:

- Implemented the Document Labeling Program requiring users across the entire organization to label documents and emails.
- Completed its effort to apply the RMF to all systems and applications previous authorized using legacy accreditation processes.

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 effect 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 Needs to Fully Implement a Software Inventory Automation Program to Manage End-of-Life and End-of-Service Assets
- The FDIC's Supply Chain Risk Management Program Lacks Maturity
- The FDIC Did Not Remove Accounts Belonging to Separated Personnel in a Timely Manner
- The FDIC Did Not Configure Privileged Accounts in Accordance with Least Privilege
- The FDIC Needs to Enforce Cybersecurity and Privacy Awareness Training Requirements

In addition, **Appendix II** notes two outstanding recommendations from prior FISMA reports warranting the FDIC's continued attention.

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. These activities include maintaining an inventory of systems, hardware, software, and software licenses; managing risk at the organizational, mission/business process, and information system levels; utilizing Plans of Action and Milestones (POA&M) to mitigate security weaknesses; and utilizing technology to provide a centralized view of cybersecurity risk management activities.

[8] NIST SP 800-12 (Rev.1), *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.

The FDIC implemented processes for maintaining a comprehensive and accurate inventory of information systems, hardware, software, and software licenses. We also noted that the FDIC 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 facing the FDIC to determine whether they were within established Risk Tolerance levels and the FDIC's Risk Appetite.

We noted an opportunity for improvement in the FDIC's POA&M management processes. We determined the FDIC is implementing POA&M management processes consistent with a Level 3 FISMA maturity. Specifically, the FDIC uses POA&Ms to document and prioritize its security weaknesses. However, due to (1) the 185 out of 355 open POA&Ms without an Acceptance of Risk delayed past the scheduled completion dates[11] (about 52 percent) and (2) the FDIC's determinations in its September 2022, December 2022, and March 2023 ITRAC reports that delayed POA&Ms present an increased risk and warrant further prioritization, we do not believe POA&M processes are managed and measurable consistent with the operating effectiveness seen at higher levels of FISMA maturity (Level 4+). The top reasons for delay documented by the FDIC include technological limitations and dependency on the completion of other tasks. A reduction in the number and average age of the delayed POA&Ms is advised to reach a higher FISMA maturity level; however, we do not believe a recommendation is warranted as the FDIC is actively remediating the issue.

Additionally, the FDIC's software asset management processes needed improvement, as noted below.

The FDIC Needs to Fully Implement a Software Inventory Automation Program to Manage End-of-Life and End-of-Service Assets

An effective software asset management system helps organizations inventory and assess the state of installed software across their IT environment, providing information about the current state of the software installed on devices that access organizational resources and support critical business functions. Organizations that automate the collection of software inventory data can better understand which software updates are needed to minimize vulnerabilities and whether vendors continue to support the software.[12]

The FDIC's platform used for EOL/EOS monitoring reported (b) (7)(E) software assets at EOL and 10,667 software assets with no available EOL data as of June 30, 2023. The CIOO stated that while it is able to generate EOL and EOS data, the data is not normalized[13] for all software products and is therefore unreliable. The CIOO is currently developing a dashboard that aims to remediate this issue by cleansing, normalizing, and correlating asset data, thereby making the data easier to find, group, and analyze. This issue was already documented in the FDIC's Risk Inventory and had a mitigation plan to address the risk item, with an estimated completion date of October 31, 2023.

[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.

[11] Identified through analysis of the entire population of POA&Ms as of February 28, 2023.

[12] https://www.nccoe.nist.gov/sites/default/files/legacy-files/sam-fact-sheet.pdf

[13] Data normalization is the practice of organizing data entries to ensure they appear similar across all fields and records, making information easier to find, group, and analyze. https://www.splunk.com/en_us/blog/learn/data-normalization.html

The lack of a fully implemented software inventory automation program impacted the relevant Risk Management metric; however, we do not believe a recommendation is warranted as the FDIC is actively remediating the issue.

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. These activities include an organization-wide SCRM strategy to manage supply chain risks; managing SCRM activities at all organization tiers; and ensuring that external providers are operating in accordance with the FDIC's cybersecurity and supply chain 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.[14]
- Modified its acquisition process to include an OCISO review of security and privacy requirements for all acquisitions; and
- Published a high-level SCRM Implementation Plan to outline the timeline for completing strategic objectives defined in the SCRM Strategy.

However, the FDIC is still developing its processes 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[15] and found that the FDIC did not implement several of its defined SCRM objectives, identify, or document its SCRM risks, or establish metrics and indicators for SCRM. The OIG issued nine recommendations that directed 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 July 28, 2023, the following five recommendations remain open:

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

[14] 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

[15] FDIC OIG Report, *The FDIC's Implementation of Supply Chain Risk Management*, March 2022 https://www.fdicoig.gov/reports-publications/audits-and-evaluations/fdics-implementation-supply-chain-risk-management

- 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 would complete corrective actions for these recommendations by June 30, 2023, but had not done so by the conclusion of our fieldwork period. The FDIC has communicated revised plans to complete corrective actions by December 31, 2023.

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. Such changes include installing software patches to address security vulnerabilities, applying software updates to improve system performance and functionality, and modifying configuration settings to strengthen security.

FISMA requires Federal agencies to ensure compliance with minimally acceptable system configuration requirements, as determined by the agency. In addition, NIST has issued guidance to help Federal agencies implement effective configuration management controls. Without effective configuration management, information systems may not operate properly, stop operating altogether, or become vulnerable to security threats.

The FDIC established policies and implemented processes for baseline configurations and patch management.[16] The FDIC also effectively deployed system configuration settings using tools that automatically enforce configuration settings, and flag misconfigurations for review and remediation. In addition, the Corporation used automated patch and vulnerability management tools, and performed tests on software patches prior to implementation. Further, the FDIC effectively implemented a vulnerability disclosure program for its internet-accessible Federal systems. Finally, the FDIC adopted the Trusted Internet Connection 3.0 (TIC) initiative[17] and developed and monitors use cases for both its on-premises and cloud implementation.

[16] 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).

[17] https://www.cisa.gov/resources-tools/programs/trusted-internet-connections-tic

Additionally, it has implemented the CISA Cloud Log Aggregation Warehouse (CLAW) solution,[18] to collect and analyze cloud security data for all of its applicable cloud environments.

However, in the FISMA report for 2022, we issued a recommendation to address the 31 POA&Ms with NIST SP 800-53 Rev. 5 control SI-2 (Flaw Remediation). As of July 28, 2023, the FDIC had taken actions to address all but two POA&Ms. The remaining two are scheduled for closure by the fourth quarter of calendar year 2023. Due to the significantly reduced count of delayed SI-2 POA&Ms, we determined the risks related to vulnerability management were reduced to an acceptable level and the impact to maturity was negated. The OIG will perform an assessment of completed corrective actions once a formal closure request is provided. Until then, this recommendation remains unimplemented.

Additionally, we noted an opportunity to improve the FDIC's implementation of baseline configuration processes. Specifically, two tools used for server scanning were missing 129 and 94 servers, respectively, from their scanning results. As a result, these two tools dropped below the 98 percent success benchmark that the FDIC established for scanning, at 92 percent and 94 percent respectively. The FDIC was unable to provide evidence that demonstrated an understanding of the cause nor follow-up actions taken by the conclusion of fieldwork. Complete populations of assets obtained through the FDIC's weekly scanning reconciliation process are critical for ensuring all devices within its environment are subject to configuration and vulnerability scans. Remediation of the scanning discrepancies will help to improve the maturity level to Level 4 (Managed and Measurable).

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. These capabilities involve defining and implementing Identity, Credential, and Access Management (ICAM) strategies, policies, procedures, and roadmaps that address Federal guidance.[19] ICAM also involves issuing and maintaining user credentials (usernames and passwords), executing non-disclosure and confidentiality agreements, and managing logical and physical access privileges.

The FDIC established a number of identity and access management controls that were consistent with FISMA requirements, OMB policy, and applicable NIST standards and guidelines. Such controls included the creation of an ICAM Strategy and Segment Architecture,[20] and policies and procedures for identifying, authenticating, and managing users who access FDIC information systems and facilities.[21] In addition, it has implemented effective multifactor authentication mechanisms for both non-privileged and privileged users for authentication to organizational resources. Further, the FDIC configured end-user devices with

[18] https://www.cisa.gov/sites/default/files/publications/NCPS%20Cloud%20Interface%20RA%20Volume%20One%20%282021-05-14%29.pdf See Section 6.1.

[19] OMB Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management* (May 2019).

[20] The ICAM Strategy is intended to lay a foundation and key initiatives for a comprehensive and integrated approach to ICAM at the FDIC. The ICAM Program Charter establishes the structure and governance for the ICAM Program, including its goals. The ICAM Segment Architecture provides the technical framework, goals, and objectives for the ICAM program.

[21] 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).

cryptographic remote access controls that restrict the ability to transfer data to non-authorized devices.

However, the FDIC's management of user accounts still needed improvement, as noted below.

The FDIC Did Not Remove Accounts Belonging to Separated Personnel in a Timely Manner

User account management involves the process of requesting, establishing, issuing, and closing user accounts; tracking users and their respective access authorizations; and managing these functions. When user accounts are no longer required, the supervisor should inform the system or application owner so accounts are removed in a timely manner.[22] The FDIC established policies in Directive 1360.15 *Access Control for Information Technology Resources*, dated January 2023, that state access to IT resources should remain active only while an authorized user is employed by the FDIC. Users should not have access before they begin work, and access should be terminated immediately after separation from the FDIC.

The FDIC also established policies in Directive 2150.1 *Pre-Exit Clearance for Employees*, that require a separating user's Immediate Supervisor to review and certify applicable sections in the Form 2150/01 *Pre-Exit Clearance Record For Employees.* The FDIC has similar processes in place for contractors, with the contract Oversight Manager taking the role of the supervisor. The Directive also establishes a policy that requires the FDIC's DIT to revoke separated employees' system access and privileges and certify applicable sections on Form 2150/01.

We noted weaknesses in the user separation process, which is a key element of the FDIC's ICAM goal to strengthen the security of the FDIC's information resources. We tested accounts belonging to a sample of 44 employees and contractors who separated from the FDIC between January 1 and May 26, 2023. Among the 44 individuals, we noted the following:

- Four users (three employees and one contractor) were removed from the network more than one business day after their effective separation date. The access for the four accounts was removed between 4 and 84 days after the user separation date.
- A fifth user (a contractor) with two accounts retained access to the network for one month after separating from the organization. One of the accounts provided privileged access. The FDIC removed access from the account with privileged access one month after user separation and the account with regular access 2 months after user separation.

The user separation process comprises multiple steps and differs for employees and contractors. For contractors, the Oversight Manager is notified of separation, completes a Pre-Exit Clearance Form, and submits an ARCS request to remove user access. For employees, their Supervisor and Administrative Officer/designee is notified of a separation and they in turn notify appropriate points of contact in the Pre-Exit Clearance Form, including the HR Specialist. The collective actions of these individuals prompt the FDIC HR system, Corporate Human Resources Information System (CHRIS), to notify ARCS to disable the user's access. For the five users in question, delays in the notification process resulted in their accounts not being

[22] Section 10.2.1, User Account Management. https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter10.html

removed timely relative to their effective separation date. We were able to confirm that at least two of the five total users returned their physical access token in a timely manner, reducing the risk of authorized access due to the implementation of multifactor authentication. Nevertheless, not removing user account access immediately upon separation leaves additional and unnecessary access points to FDIC data, increasing the risk to data confidentiality and integrity.

We recommend the FDIC:

1. Implement process improvements to ensure prompt notification and removal of user network accounts on or before the user's separation date.

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 privileged accounts within networks and information systems. Privileged accounts have elevated access privileges that can bypass system controls and access sensitive system resources. For these reasons, privileged 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, privileged accounts must be carefully provisioned, monitored, and deactivated when no longer necessary.

The FDIC uses a directory service called Active Directory to manage user privileges across the organization. The FDIC employs a Role-Based Access Control system in which it defines a list of roles, each with a set of system permissions, that are configured in Active Directory. 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 administrative roles that are considered privileged.

The OIG published its report on *The FDIC's Security Controls Over Microsoft Windows Active Directory* in March 2023. The objective of this audit was to assess whether the FDIC designed and implemented effective controls for the Active Directory to protect network systems and data. The OIG identified instances in which accounts were configured with elevated account settings; however, there was no justification provided for such settings, and the elevated settings were not 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.

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. Organizations must consider the protection of PII over its lifecycle (from initial acquisition through disposal), including the confidentiality, integrity, and availability of PII using controls such as encryption, data loss prevention, labeling, and minimizing PII holdings.

The FDIC established a number of data protection and privacy controls that were consistent with FISMA requirements, OMB policy, and applicable NIST standards and guidelines. Such controls included the maintenance of Privacy Impact Assessments (PIA),[23] a Privacy Program Plan, an inventory of PII at the FDIC, the establishment of data encryption, and the integration of Privacy into the ISCM strategy. The FDIC also employs mechanisms, such as firewalls, email authentication technology, and Data Loss Prevention (DLP) tools, to detect and minimize exfiltration of information.

The FDIC also completed corrective actions for an audit recommendation issued in our FISMA report for 2021 related to implementing its document labeling guide requirements across the organization. Specifically, the FDIC implemented tool-based requirements for sensitivity labels on all electronic documents and communications. The OIG closed this recommendation on July 6, 2023.

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. According to FISMA, the purpose of such training is to inform personnel of the information security risks associated with their activities, and their responsibility to comply with agency policies and procedures designed to reduce these risks. FISMA also requires agencies to report on the resources, including budget, staffing, and training, necessary to implement an agency security program.

The FDIC established policies, including FDIC Circulars 1360.16, *Mandatory Cybersecurity and Privacy Awareness Training* (April 2023) and 1360.9, *Protecting Information* (July 2023), which require all FDIC employees and contractor personnel with network access to complete Cybersecurity and Privacy Awareness Training (CPAT). This requirement is intended to raise awareness among network users of computer security and privacy laws, regulations, and policies; rules of behavior and effective security practices; and requirements governing the FDIC's collection, use, sharing, and protection of information according to its sensitivity. The FDIC also developed a Workforce Planning Guide that documents the need to perform periodic workforce assessments. Doing so would allow CIOO senior management to determine personnel competencies and skill gaps within a continuously changing IT environment. The CIOO could then take actions to address the skill gaps identified in the assessment. The FDIC was actively planning an assessment as of the end of our fieldwork period.

However, the FDIC's security training program needed improvement, as noted below.

The FDIC Needs to Enforce Cybersecurity and Privacy Awareness Training Requirements

A robust and enterprise-wide awareness and training program is paramount to ensuring that people understand their security responsibilities, organizational policies, and how to properly use and protect the information and systems entrusted to them. The FDIC relies on information systems to support its mission and thus provides system access to FDIC employees and contractors ("users") accordingly to perform their job functions.

[23] According to NIST SP 800-37 (Rev. 2) *Risk Management Framework for Information Systems and Organizations*, a privacy impact assessment is an analysis about how an organization handles PII in accordance with applicable legal, regulatory, and policy requirements.

On March 7, 2023, the FDIC published a new CPAT and required all users to complete the training by June 30, 2023. FDIC Circular 1360.16 also requires FDIC employees and contractors to complete the CPAT within 5 business days of receiving FDIC equipment, and annually thereafter. The OCISO tracks training compliance in its learning management system and revokes user access if an individual fails to complete training in a timely manner. It revokes user access by manually moving the users into an Active Directory group[24] that limits user network access until they complete the required training.

On July 12, 2023, we obtained a training compliance report listing over 400 personnel who did not complete the new training by the June 30, 2023 deadline. In addition, most of the individuals were not added to the Active Directory group that is used to enforce compliance with training requirements by limiting user network access to the learning management system only. The FDIC attributed this to the fact that users in the Active Directory group who access the FDIC network via Virtual Private Network (VPN) cannot access its learning management system, FLX,[25] to complete the training. Therefore, the FDIC did not add users into that group. As of July 28, 2023, the FDIC is working to fix this issue so that it can enforce access restrictions for individuals that did not complete the training. In the meantime, the FDIC is sending emails three times a week to users and their supervisors to remind them about training requirements.

We recommend the FDIC:

2. Address the technical issues preventing enforcement of security and privacy training compliance.

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[26] include anomalies and changes in the organization's IT environment that may impact organizational operations, including mission, capabilities, or reputation.

Information Security Continuous Monitoring

The *Information Security Continuous Monitoring* Domain includes controls that address an agency's maturity in implementing an ISCM strategy and governance structure, granting system authorizations, performing system assessments, and monitoring systems on an ongoing basis.

NIST SP 800-137, *Information Security Continuous Monitoring 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.

[24] Active Directory security groups are a way to collect accounts into manageable units. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups

[25] The FDIC transitioned to FLX in September 2022.

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

The FDIC established and implemented policies and guidance to support the continuous monitoring of its information systems.[27] The FDIC followed the steps from the NIST RMF to authorize information systems with an authorization to operate (ATO)[28] 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 2021 related to ensuring that its operational systems and subsystems were subject to the NIST RMF assessment and authorization processes. Specifically, the FDIC completed efforts to apply the RMF to 151 systems and subsystems previously authorized using legacy accreditation processes. The OIG closed this recommendation on June 7, 2023.

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

The *Incident Response* Domain includes controls that address an agency's maturity in implementing technologies for detecting, analyzing, and handling security incidents.

FISMA requires each agency to develop, document, and implement an agency-wide information security program that includes policies and procedures for incident response. In addition, NIST SP 800-61, *Computer Security Incident Handling Guide,* Rev. 2, defines procedures for acquiring necessary tools and resources; detecting, analyzing, and reporting incidents; containing, eradicating, investigating, and recovering from incidents; and capturing lessons learned to improve incident response processes.

The FDIC established policies and procedures for responding to computer security incidents;[29] issued an 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 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). The FDIC signed a Memorandum of Agreement (MOA) with DHS to augment its intrusion detection and response capabilities. The FDIC also established its own incident response capabilities, which included firewalls, intrusion detection, and endpoint security tools. These tools were integrated with a Security Incident and Event

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

[28] 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.

[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.

Management (SIEM) tool to provide the FDIC with a holistic view of potential incidents across the organization.

As stated in the "Event Logging" description under DHS FISMA Reporting Metrics and the NIST Cybersecurity Framework, OMB M-21-31 requires agencies to improve their event logging and log management capabilities along three maturity levels (EL1, EL2, and EL3). As of July 28, 2023, the FDIC demonstrated EL1 maturity. Although it was behind the timeline outlined in M-21-31 (Achieve EL2 maturity by February 27, 2023), we acknowledged that this delay was partially due to a dependency on the release of CISA guidance not yet published at the conclusion of our fieldwork period. Without the CISA guidance, the FDIC would be unable to fully comply with EL2 requirements. Therefore, we are not issuing a recommendation addressing this issue. The FDIC is working on fulfilling the other requirements for achieving EL2 maturity, including to ensure that all required system logs are retained in acceptable formats for specified timeframes.

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

The *Contingency Planning* Domain includes controls that address an agency's maturity in implementing a governance structure over system contingency planning activities, performing business impact analyses, maintaining system contingency plans, testing those contingency plans through simulated exercises, and communicating system recovery information to relevant stakeholders.

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 defined key points of contact necessary to implement its contingency planning strategy and performed Business Impact Analyses to calculate the system criticality for our two in-scope systems used by the FDIC (see selection criteria for the two systems in **Appendix I**). In addition, in October 2022 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 an entirely remote environment. 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. The AAR noted that all 45 tested applications failed over and back within the required time period. The AAR included 30 follow-up actions designed to improve documentation requirements, enhance communication between test personnel, and troubleshoot technical concerns identified during the test.

[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.

CONCLUSION

The FDIC established several controls and practices consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines. Our report contains two recommendations and cites two 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 – OBJECTIVE, SCOPE, AND METHODOLOGY

Cotton conducted this performance audit, with FDIC OIG oversight, 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 5 components of internal control, and 16 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) 2023-2024 IG 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 July 28, 2023 (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-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements* (December 2022), when planning and conducting our work. We also consulted the FY 2023 FISMA Metrics Evaluator's Guide to verify the reasonableness of our procedures.
- 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. Our analysis of these systems included reviewing selected system documentation and other relevant information, as well as testing selected security controls. We selected these systems because they support mission-essential functions.[33] A disruption of their operation could impair the FDIC's business

[32] The Green Book organizes internal control through a hierarchical structure of 5 components and 17 principles. The five 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.

[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.

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 2023.

APPENDIX II – STATUS OF PRIOR-YEAR FISMA RECOMMENDATIONS

The following table summarizes the OIG's determinations regarding the status of previously unaddressed recommendations from FISMA audit reports issued in 2021 and 2022. Recommendations marked 'Closed' denote Status updates that followed the publication of the FISMA report in 2022.

Recommendation	Status
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 4 Implement Document Labeling Guide requirements across the entire organization as dictated by business needs.	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.	Closed
Report Issued in 2022, Recommendation 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).	Unimplemented

APPENDIX III – LIST OF ACRONYMS

Acronym	Description
AAR	After Action Report
ATO	Authorization to Operate
CDM	Continuous Diagnostics and Mitigation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
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 & Resolution
CPAT	Cybersecurity and Privacy Awareness Training
CPO	Chief Privacy Officer
CSIRT	Computer Security Incident Response Team
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
DOF	Division of Finance
DRR	Division of Resolutions and Receiverships
EDR	Endpoint Detection and Response
EO	Executive Order
EOL	End-of-Life
EOS	End-of-Service
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
GFE	Government Furnished Equipment
ICAM	Identity, Credential, and Access Management
IG	Inspector General
ISCM	Information Security Continuous Monitoring
ISM	Information Security Manager
ISSM	Information System Security Manager
IT	Information Technology
ITRAC	IT Risk Advisory Council
Legal	Legal Division
MEF	Mission Essential Function

MOA	Memorandum of Agreement
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 & Internal Controls
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
RBAC	Role-Based Access Control
RMF	Risk Management Framework
RMS	Division of Risk Management Supervision
SAOP	Senior Agency Official for Privacy
SCRM	Supply Chain Risk Management
SIEM	Security Incident and Event Management
SOC	Security Operations Center
SOP	Standard Operating Procedure
SP	Special Publication
SRT	Security Response Team
US-CERT	United States Computer Emergency Readiness Team

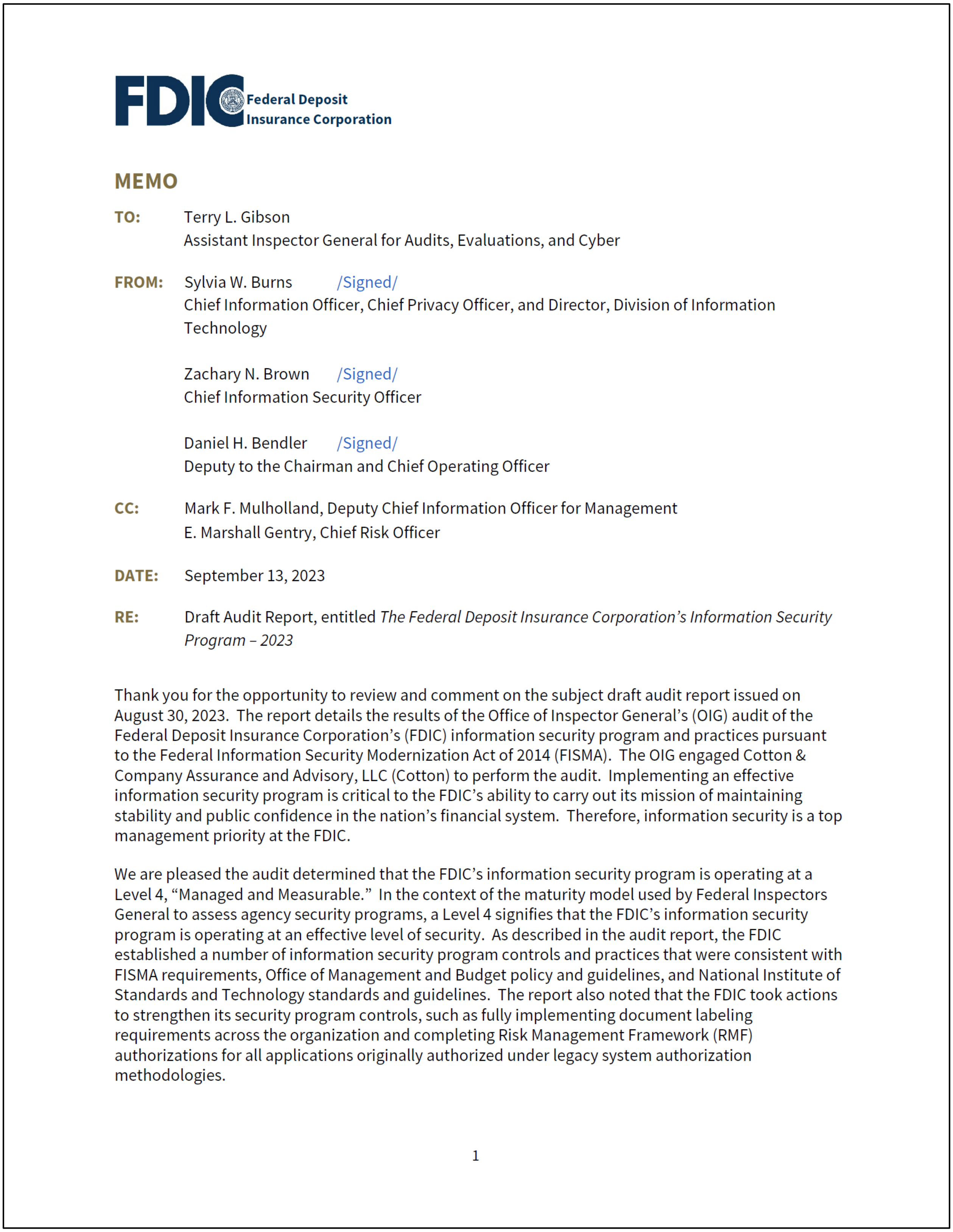
Part II

****

FDIC Comments and OIG Evaluation

FDIC Comments and OIG Evaluation

The FDIC's Chief Information Officer, Chief Information Security Officer, and Chief Operating Officer provided a written response, dated September 13, 2023, to a draft of the report. The response is presented in its entirety beginning on page II-2. In the response, the FDIC concurred with the report's recommendations. The recommendations will remain open until we confirm that corrective actions have been completed and are responsive. A summary of the FDIC's corrective actions is presented on page II-4.



FDIC Federal Deposit Insurance Corporation

MEMO

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

FROM: Sylvia W. Burns /Signed/
Chief Information Officer, Chief Privacy Officer, and Director, Division of Information Technology

Zachary N. Brown /Signed/
Chief Information Security Officer

Daniel H. Bendler /Signed/
Deputy to the Chairman and Chief Operating Officer

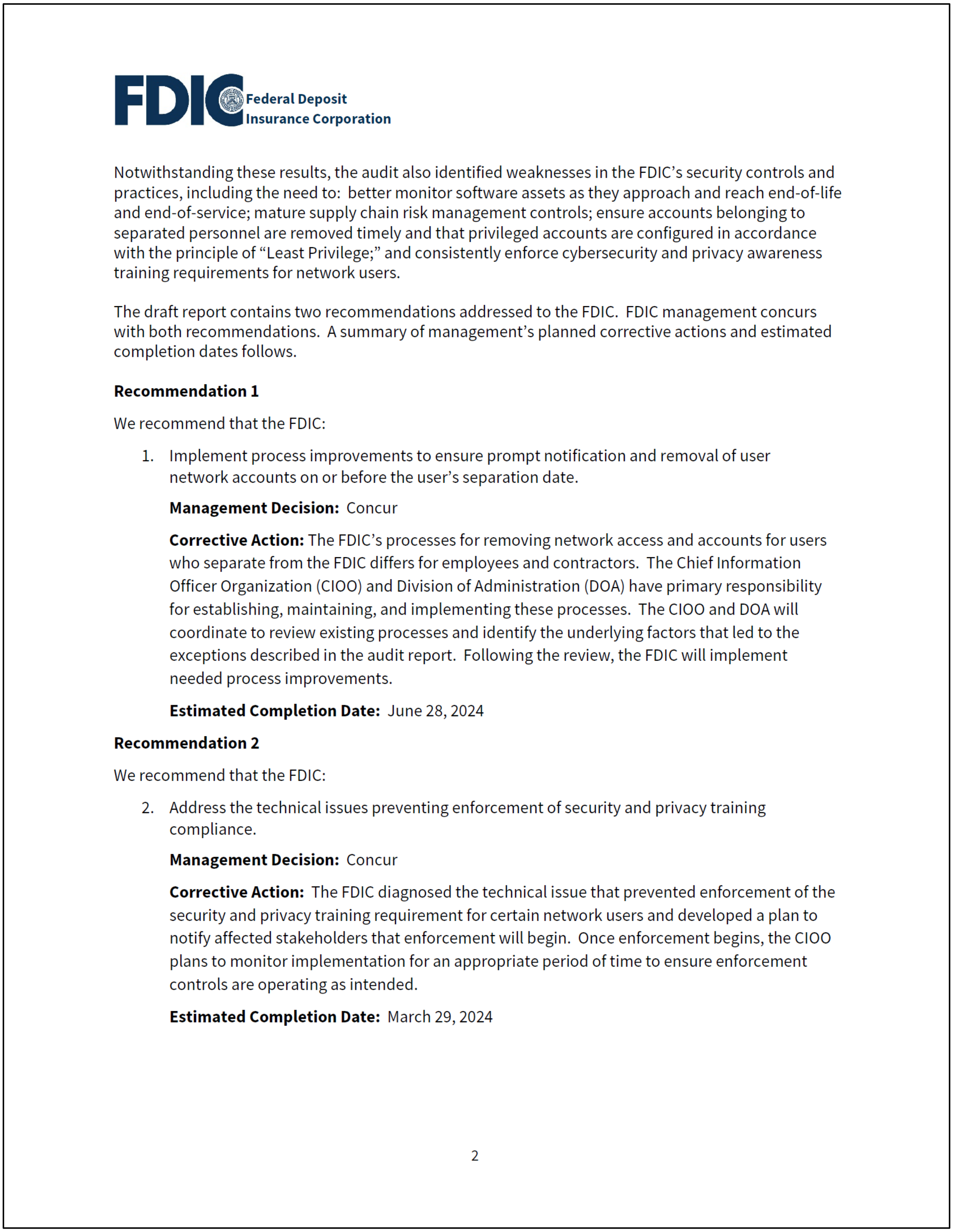
CC: Mark F. Mulholland, Deputy Chief Information Officer for Management
E. Marshall Gentry, Chief Risk Officer

DATE: September 13, 2023

RE: Draft Audit Report, entitled *The Federal Deposit Insurance Corporation's Information Security Program – 2023*

Thank you for the opportunity to review and comment on the subject draft audit report issued on August 30, 2023. The report details the results of the Office of Inspector General's (OIG) audit of the Federal Deposit Insurance Corporation's (FDIC) information security program and practices pursuant to the Federal Information Security Modernization Act of 2014 (FISMA). The OIG engaged Cotton & Company Assurance and Advisory, LLC (Cotton) to perform the audit. Implementing an effective information security program is critical to the FDIC's ability to carry out its mission of maintaining stability and public confidence in the nation's financial system. Therefore, information security is a top management priority at the FDIC.

We are pleased 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 to assess agency security programs, a Level 4 signifies that the FDIC's information security program is operating at an effective level of security. As described in the audit report, the FDIC established a number of information security program controls and practices that were consistent with FISMA requirements, Office of Management and Budget policy and guidelines, and National Institute of Standards and Technology standards and guidelines. The report also noted that the FDIC took actions to strengthen its security program controls, such as fully implementing document labeling requirements across the organization and completing Risk Management Framework (RMF) authorizations for all applications originally authorized under legacy system authorization methodologies.



FDIC Federal Deposit Insurance Corporation

Notwithstanding these results, the audit also identified weaknesses in the FDIC's security controls and practices, including the need to: better monitor software assets as they approach and reach end-of-life and end-of-service; mature supply chain risk management controls; ensure accounts belonging to separated personnel are removed timely and that privileged accounts are configured in accordance with the principle of "Least Privilege;" and consistently enforce cybersecurity and privacy awareness training requirements for network users.

The draft report contains two recommendations addressed to the FDIC. FDIC management concurs with both recommendations. A summary of management's planned corrective actions and estimated completion dates follows.

Recommendation 1

We recommend that the FDIC:

1. Implement process improvements to ensure prompt notification and removal of user network accounts on or before the user's separation date.

   Management Decision: Concur

   Corrective Action: The FDIC's processes for removing network access and accounts for users who separate from the FDIC differs for employees and contractors. The Chief Information Officer Organization (CIOO) and Division of Administration (DOA) have primary responsibility for establishing, maintaining, and implementing these processes. The CIOO and DOA will coordinate to review existing processes and identify the underlying factors that led to the exceptions described in the audit report. Following the review, the FDIC will implement needed process improvements.

   Estimated Completion Date: June 28, 2024

Recommendation 2

We recommend that the FDIC:

2. Address the technical issues preventing enforcement of security and privacy training compliance.

   Management Decision: Concur

   Corrective Action: The FDIC diagnosed the technical issue that prevented enforcement of the security and privacy training requirement for certain network users and developed a plan to notify affected stakeholders that enforcement will begin. Once enforcement begins, the CIOO plans to monitor implementation for an appropriate period of time to ensure enforcement controls are operating as intended.

   Estimated Completion Date: March 29, 2024

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 and DOA will coordinate to review existing processes and identify the underlying factors that led to the exceptions described in the audit report. Following the review, the FDIC will implement needed process improvements.	June 28, 2024	$0	Yes	Open
2	The FDIC diagnosed the technical issue that prevented enforcement of the security and privacy training requirement for certain network users and developed a plan to notify affected stakeholders that enforcement will begin. Once enforcement begins, the CIOO plans to monitor implementation for an appropriate period of time to ensure enforcement controls are operating as intended.	March 29, 2024	$0	Yes	Open

[a] Recommendations are resolved when —

1. Management concurs with the recommendation, and the OIG agrees the planned corrective action is consistent with the recommendation.
2. Management does not concur or partially concurs with the recommendation, but the OIG agrees that the proposed corrective action meets the intent of the recommendation.
3. For recommendations that include monetary benefits, management agrees to the full amount of OIG monetary benefits or provides an alternative amount and the OIG agrees with that 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.

FDIC OIG website	X, formerly known as Twitter	OVERSIGHT.GOV ALL FEDERAL INSPECTOR GENERAL REPORTS IN ONE PLACE
www.fdicoig.gov	@FDIC_OIG	www.oversight.gov/