Office of Inspector General

The FDIC's Information Security Program – 2021

October 2021 **AUD-22-001**

Audit Report

Audits, Evaluations, and Cyber

REDACTED VERSION

PUBLICLY AVAILABLE

Portions of this report containing sensitive information have been redacted and are marked accordingly.

Integrity✰Independence✰Accuracy✰Objectivity✰Accountability

Executive Summary

The FDIC's Information Security Program – 2021

The Federal Information Security Modernization Act of 2014 (FISMA), Public Law No. 113-283, requires Federal agencies, including the Federal Deposit Insurance Corporation (FDIC), to conduct annual independent evaluations of their information security programs and practices and to report the results to the Office of Management and Budget (OMB). FISMA requires independent evaluations to be performed by the agency Inspector General (IG), or an independent external auditor as determined by the IG. The FDIC Office of Inspector General (OIG) engaged the professional services firm of Cotton & Company LLP (Cotton & Company) to conduct this audit.

The objective of the audit was to evaluate the effectiveness of the FDIC's information security program and practices. Cotton & Company planned and conducted its work based on the Department of Homeland Security's (DHS) reporting metrics: *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.1* (May 2021) (DHS FISMA Metrics).

The DHS FISMA Metrics require IGs to assess the effectiveness of the agency's information security programs and practices using a maturity model. This maturity model aligns with the five function areas in the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*: Identify, Protect, Detect, Respond, and Recover. IGs must assign maturity level ratings to each of the five function areas, as well as an overall rating, using a scale of 1-5, where 5 represents the highest level of maturity.[1] Maturity ratings are determined by a simple majority where the most frequent level (mode) across the component questions will serve as the domain rating.

Results

Applying the DHS FISMA Metrics, Cotton & Company determined that the FDIC's overall information security program was operating at a Maturity Level 4. In reaching this determination, we are constrained by the methodology and limitations as

[1] The five maturity level ratings are (1) Ad Hoc, (2) Defined, (3) Consistently Implemented, (4) Managed and Measurable, and (5) Optimized. In general, lower level maturity ratings (1-2) focus on defining policies, procedures, and strategies, while higher level ratings (4-5) focus on measuring and optimizing performance. Information security programs with Maturity Levels 4 and 5 are considered to be operating at effective levels of security.

required by the DHS FISMA Metrics. This mode-based methodology does not seem to fully capture the nature, scope, and magnitude of the risk posture of an agency's IT security, because it requires the agency to receive the higher rating when there are an equal number of ratings at different levels.[2] In cases where there is a tie for the most frequent rating, the DHS FISMA Metrics indicate that the agency will be rated at the higher level, even where there is a wide disparity among ratings. The same mode-based scoring system applies at the function area level to calculate the overall agency rating.

In addition, this numerical score should not be compared to prior or future years, since the DHS FISMA Metrics have shifted over time. These changes, together with differences in the scope of audit work performed each year, make it imprudent to compare this year's maturity level ratings to ratings in both prior and future years. The table below presents the maturity level ratings Cotton & Company assigned to the five function areas and to the overall program.

Function Area	Rating
Identify	3
Protect	4
Detect	2
Respond	4
Recover	4
Overall Rating	**4**

During the past year, the FDIC had established certain information security program controls and practices. In addition, the FDIC worked to strengthen its security controls following the issuance of our FISMA 2020 audit report. Specifically, the FDIC updated its Privacy Program; created processes to prevent unauthorized software from being installed on the FDIC network; reviewed Risk Acceptance decisions; defined and implemented the oversight authorities, roles, and responsibilities of its Operating Committee; enhanced procedures for employee and contractor investigations; updated contingency planning policies and procedures; and conducted tests of the contingency plan.

However, the audit report describes significant security control weaknesses that reduced the effectiveness of the FDIC's information security program and practices and that can be improved to reduce the impact to the confidentiality, integrity, and availability of the FDIC's information systems and risk to data. The FDIC should ensure a proper sense of urgency and expediency to proactively address and resolve weaknesses in its information security program, including the most significant risks as identified by Cotton & Company and described below:

[2] For example, if there are seven questions in a domain, and the agency receives Level 1 ratings for three component questions and Level 5 ratings for four component questions, then the DHS FISMA Metrics requires that the domain rating be at a Level 5 (Optimized) – even though three ratings were at an Ad Hoc level (Level 1) and represented significant weaknesses in IT security.

High Number of Overdue and Unaddressed High- and Moderate-Risk Plans of Action and Milestones (POA&Ms) (Identify – Risk Management). In July 2021, we analyzed the entire population of open POA&Ms in the Cyber Security Assessment and Management system. We found that there were 176 high- and moderate-risk open POA&Ms and the scheduled completion dates ranged from March 2010 to July 2021. Without consistently addressing control deficiencies timely, the FDIC will continue to face an increasing backlog of POA&Ms, leaving its data more vulnerable to security exploits from unmitigated threats.

The FDIC's Supply Chain Risk Management Program Lacks Maturity (Identify – Supply Chain Risk Management (SCRM)). Federal agencies are required to develop and implement plans and strategies to assess and monitor their supply chain risks. In addition, they are responsible for integrating supply chain risk management practices throughout the lifecycle of each system, component, service, or asset.

While the FDIC established a directive that contains elements of an SCRM strategy, the FDIC has not defined processes and procedures that support the underlying components of the directive. Without SCRM processes and procedures, the FDIC cannot be sure that its products, system components, systems, and services provided by external parties are maintained consistently with its cybersecurity requirements, thus placing it at increased risk of exploitation through its supply chain.

Administrative Account Management Needs Improvement (Protect – Identity and Access Management). Administrative Accounts are highly sought-after targets by hackers and other adversaries who may wish to use the accounts to corrupt data, launch attacks, or conduct other malicious activities. As a result, Administrative Accounts must be carefully provisioned, monitored, and deactivated when no longer necessary.

We have reported weaknesses related to Administrative Account management in each of our past four FISMA audit reports issued since 2017, and during FY 2021, we identified 10 additional open POA&Ms related to privileged user access. Weaknesses in the FDIC's processes for managing Administrative Accounts increase the risk of unauthorized activity, such as individuals accessing, modifying, deleting, or exfiltrating sensitive information. In light of repeated weaknesses in this area, the FDIC should take steps to identify the underlying causes of the Administrative Account management weaknesses and take action to strengthen associated controls as we recommended in our FY 2020 FISMA report.

Inadequate Oversight and Monitoring of FDIC Information Systems (Detect – Information Security Continuous Monitoring). Historically, several systems, components, and services that should have been assessed according to the NIST Risk Management Framework (RMF) process were instead mischaracterized as subject to the now-rescinded *Outsourced Solution Assessment Methodology*. As a result, the FDIC did not subject these systems to a proper risk assessment, authorization to operate (ATO), or ongoing monitoring in accordance with the RMF.

As of June 22, 2021, the FDIC had not yet completed the ATO for 10 operational systems. Until the FDIC subjects all of its systems, internal or outsourced, to the RMF, the FDIC cannot be sure it will identify and address security and privacy risks in a timely manner.

Recommendations

The audit report contains six recommendations for the FDIC to develop and implement SCRM processes and procedures in accordance with the Supply Chain Risk Management Program Directive and applicable government guidance; begin tracking completion of the Identity, Credential, and Access Management (ICAM) milestones of its revised ICAM Roadmap; fully implement the Privacy Continuous Monitoring process to include updating Privacy Impact Assessments for all required systems; implement Document Labeling Guide requirements across the organization; analyze the Document Labeling Guide for previously-created documents; and ensure that the FDIC's information systems are subject to a formal authorization process.

Contents

Part I

Part II

Part I

☆☆☆☆☆☆☆☆

Report by Cotton & Company LLP

The Federal Deposit Insurance Corporation's Information Security Program – 2021

Audit Report

October 27, 2021

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

TABLE OF CONTENTS

Cotton& Company
Answers Questioned

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

Terry L. Gibson
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 – 2021

Cotton & Company LLP 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 & Company LLP to conduct this performance audit pursuant to Contract Number CORHQ-18-G-0479-0004. Cotton & Company LLP performed the work from April through September 2021.

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

Sincerely,

(b) (6)

Loren Schwartz, CPA, CISSP, CISA
Partner

INTRODUCTION

According to the Office of Management and Budget (OMB), cybersecurity remains a significant challenge in the Federal IT landscape. Notably, in December 2020, a sophisticated supply chain attack was used to gain access to a large number of information systems across several Federal Government Agencies, serving as a reminder that the Federal Government must continually invest in defensive capabilities to reduce the impact of cybersecurity incidents. OMB reported that Federal agencies experienced 30,819 cybersecurity incidents during Fiscal Year (FY) 2020,[1] nearly an eight percent increase over the incidents reported in FY 2019.

The Federal Deposit Insurance Corporation (FDIC) relies heavily on information systems to carry out its responsibilities of insuring deposits; examining and supervising financial institutions for safety, soundness, and consumer protection; making large and complex financial institutions resolvable; and managing receiverships. These systems contain sensitive information, such as personally identifiable information (PII), including names, Social Security Numbers, and bank account numbers for FDIC employees and depositors of failed financial institutions; confidential bank examination information, including supervisory ratings; and sensitive financial data, including credit card numbers. Without effective controls for safeguarding its information systems and data, the FDIC would be at increased risk of a cyberattack that could disrupt critical operations and allow inappropriate access to, and disclosure, modification, or destruction of, sensitive information. Such an attack could threaten the FDIC's ability to accomplish its mission of ensuring the safety and soundness of institutions and maintaining stability and public confidence 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 the National Institute of Standards and Technology (NIST) to develop risk-based standards and guidelines to assist agencies in defining security requirements for their information 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:

- 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

[1] OMB, *Federal Information Security Modernization Act of 2014 Annual Report to Congress*, Fiscal Year 2020.
[2] Pub. L. No. 113-283 (December 2014). FISMA's obligations for Federal agencies and for Federal Inspectors General, as relevant to this audit, are codified chiefly to 44 U.S.C. §§ 3554 and 3555, respectively. The FDIC has determined that FISMA is legally binding on the FDIC.

- 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.

The President's Executive Order 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.

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

AUDIT OBJECTIVE

The objective of this performance audit was to evaluate the effectiveness of the FDIC's information security program and practices. We considered FISMA requirements, NIST security standards and guidelines, the NIST Cybersecurity Framework, policy and guidance issued by OMB, FDIC policies and procedures, and DHS guidance and reporting requirements to plan and perform our work and to conclude on our audit objective.

SCOPE AND METHODOLOGY

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

We assessed internal controls that we deemed significant to the audit objective. Specifically, we assessed 5 components of internal control, and 17 associated principles as defined in the Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* (September 2014) (Green Book).[4] However, the scope of our assessment of internal controls was limited to the DHS *Fiscal Year (FY) 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.1* (May 12, 2021) (DHS FISMA Reporting Metrics), which we used to assess the effectiveness of the FDIC's information security program and practices. Accordingly, our work may

[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.

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

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 8, 2021 (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-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements* (November 2020), when planning and conducting our work.

- Assessed the maturity of the FDIC's information security program with respect to the metrics defined in the DHS FISMA Reporting Metrics. As discussed later, 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 Office of Inspector General (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, (b) (7)(E) and (b) (7)(E), and one contractor system, *MyEnroll*. Our analysis of these systems included reviewing selected system documentation and other relevant information, as well as testing selected security controls. The systems are described below:

FDIC-Maintained Information Systems

- (b) (7)(E)
  (b) (7)(E) is a Commercial off the Shelf (COTS) document management product that allows the FDIC to control access to and maintain version control for documents stored on the application. It includes attributes such as check-in, check-out, workflow, and version management. There are 10 FDIC applications that are based on (b) (7)(E) to store content. These applications support a range of business functions throughout the FDIC. For example, certain mission-critical or mission-essential applications utilize (b) (7)(E) to store bank closing records and resolution plans for financial institutions.
- (b) (7)(E)
  (b) (7)(E) provides hosting platform services for FDIC applications, software, and Enterprise Services that are required for FDIC operations. These platforms are hosted in FDIC secure data centers. (b) (7)(E) provides and maintains the (b) (7)(E) operating systems and platforms that comprise the underlying infrastructure, and consists of a mix of virtual and hardware with (b) (7)(E) operating systems.

Contractor System

- *MyEnroll*
  MyEnroll is an external website operated by Benefit Allocation Systems (BAS), Inc. The website allows FDIC employees to self-enroll and update their employment benefit elections such as Dental Insurance and Life Insurance.

We selected the systems described above because they contain large quantities of sensitive information and/or support mission-essential functions.[5] A disruption of (b) (7)(E) could impair the FDIC's access to resolution plans and services necessary for operations, ultimately hindering the FDIC's ability to achieve its mission while a disruption of MyEnroll could impact FDIC employees' ability to update their benefit information.

Cotton & Company LLP conducted the audit remotely at its off-site locations in the Washington, D.C. metropolitan area from April through September 2021.

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 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 Inspectors General (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 consistency among IG FISMA evaluations. The DHS FISMA Reporting Metrics divide the five function areas into nine domains. Table 1 below illustrates the alignment of the function areas with the domains.

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

Function Area	Function Area Objective	Domain(s)
Identify	Develop an organizational understanding of the business context and the resources that support critical functions to manage cybersecurity risk to systems, people, assets, data, and capabilities.	**Risk Management and Supply Chain Risk Management**
Protect	Implement safeguards to ensure delivery of critical infrastructure services, as well as to prevent, limit, or contain the impact of a cybersecurity event.	**Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training**

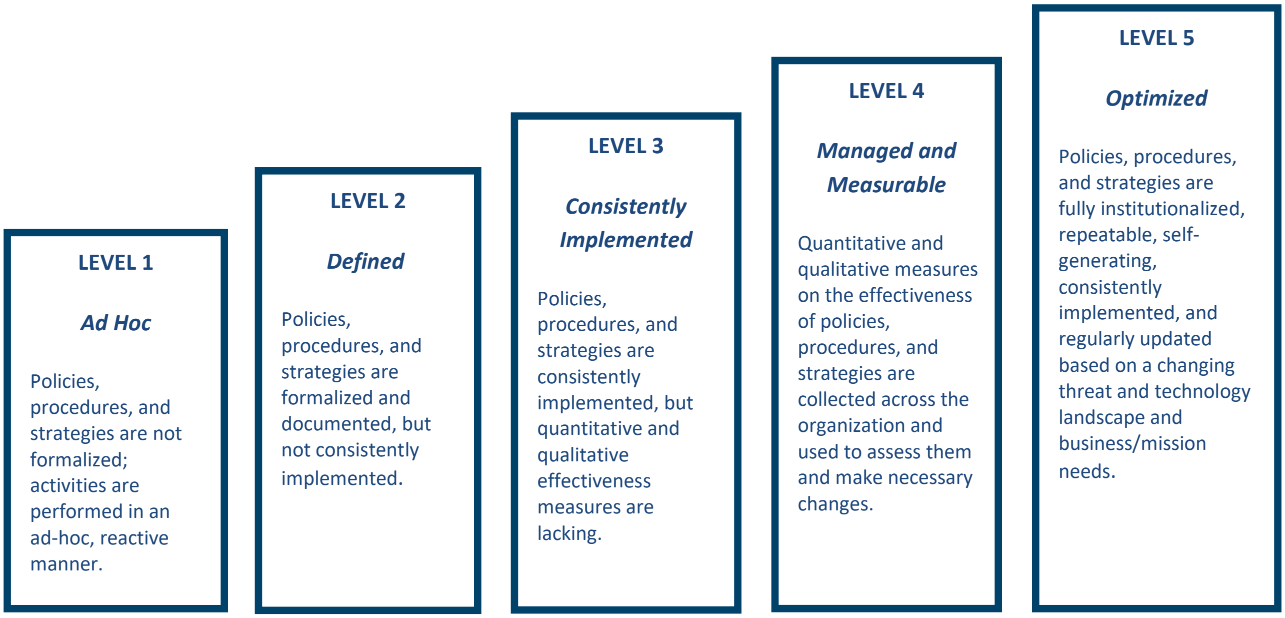
[5] According to FDIC Directive 1360.13, *IT Continuity Implementation Program*, a Mission Essential Function (MEF) is directly related to accomplishing an organization's mission as set forth in its statutory or executive charter. Any IT application, system, or service that supports a MEF is deemed "mission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

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 & Company LLP analysis of the NIST Cybersecurity Framework and DHS FISMA Reporting Metrics.

The DHS FISMA Reporting Metrics require IGs to assess the effectiveness of their agency's information security program and practices using a maturity model. Figure 1 describes the five levels of the maturity model: *Ad Hoc*, *Defined*, *Consistently Implemented*, *Managed and Measurable*, and *Optimized*. Maturity Level 1 (*Ad Hoc*) and Level 2 (*Defined*) are considered foundational, while Maturity Level 4 (*Managed and Measurable*) and Level 5 (*Optimized*) are considered advanced. According to the DHS FISMA Reporting Metrics, the foundational maturity levels ensure that agencies develop sound policies and procedures, and the advanced levels capture the extent to which agencies institutionalize those policies and procedures. Maturity Level 3 (*Consistently Implemented*) indicates that the organization has policies and procedures in place but must strengthen its quantitative and qualitative effectiveness measures for its security controls. Within the context of the maturity model, a Maturity Level 4 (*Managed and Measurable*) information security program is considered to be operating at an effective level of security.[6]

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.

Ratings throughout the nine domains are determined by a simple majority, here the most frequent level (mode) across the component questions will serve as the domain rating. For example, if there are seven

[6] More information regarding how Inspectors General are to determine maturity level ratings can be found at https://www.cisa.gov/publication/fy21-fisma-documents.

questions in a domain, and the agency receives Level 1 ratings for three component questions and Level 5 ratings for four component questions, then the DHS Metrics requires that the domain rating be at a Level 5 (Optimized) – even though three ratings were at an Ad Hoc level (Level 1) and represented significant weaknesses in the IT security system. In cases where there is a tie for the most frequent rating, the agency will be rated at the higher level. The same mode-based scoring system applies at the function area level to calculate the overall agency rating. As a result, a high rating for a domain or function area does not preclude high-impact risks within a constituent metric.

Supply Chain Risk Management (SCRM)

The FY 2021 DHS FISMA Reporting Metrics introduced the Supply Chain Risk Management (SCRM) domain within the Identify function area. 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,[7] which directed agencies to assess, avoid, mitigate, accept, or transfer supply chain risks.

The importance of SCRM was further highlighted by the SolarWinds[8] cyberattack. On December 13, 2020, FireEye, an American cybersecurity company, announced the discovery of a highly sophisticated cyber intrusion that leveraged a commercial infrastructure monitoring software application made by SolarWinds. It was determined that advanced persistent threat[9] (APT) actors infiltrated the supply chain of SolarWinds, inserting a backdoor into the product. As customers downloaded the Trojan Horse[10] installation packages from SolarWinds, attackers were able to access the systems running the SolarWinds product(s). According to Solarwinds, this includes up to 300,000 customers, including 425 of the US Fortune 500, all five branches of the U.S. military, and multiple U.S. Federal agencies. At a minimum, this provides attackers with prolonged access to large quantities of data from these organizations. However, an attacker with the capabilities typical of APT actors can leverage their access to obtain additional access to organizational networks and further steal or compromise data while avoiding detection. The Cybersecurity and Infrastructure Security Agency (CISA) determined that this threat poses a grave risk to the Federal Government and state, local, tribal, and territorial governments. It also poses risks to critical infrastructure entities and other private sector organizations. The FDIC uses SolarWinds products; however, there was no indication that it was impacted by the attack.

Supply chain attacks are especially risky due to several factors:

1. An organization (such as the FDIC) relies on many external providers to fulfill its mission, increasing the potential attack surface.
2. External providers may have many customers, increasing their attractiveness as potential targets.
3. Attacks may be difficult to detect due to an organization's trust of external vendors.

[7] The Federal Acquisition Supply Chain Act of 2018, Title II of the SECURE Technology Act, Public Law 115-390 (2018).
[8] SolarWinds is an American company that develops IT management and performance monitoring software.
[9] According to NIST 800-39 *Managing Information Security Risk*, an advanced persistent threat is an adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (for example, cyber, physical, and deception).
[10] A Trojan Horse is malware that disguises itself as a legitimate program.

In addition to SolarWinds, there have been other supply chain attacks in 2021.

The criteria for the SCRM Metrics reference controls within NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, which was published in September 2020. The DHS FISMA Reporting Metrics state that the new SCRM Metrics should not be considered for the purposes of rating the Identify framework function so as to give agencies sufficient time to fully implement NIST 800-53 Rev 5. In alignment with this requirement, we identify the SCRM weaknesses at the FDIC in this report, but did not consider them in our calculation of the rating for the Identify framework function.

Vulnerability Disclosure Policy

The FY 2021 DHS FISMA Reporting Metrics also included a new metric within the Configuration Management Domain for Vulnerability Disclosure Policy (VDP) requirements. This metric supports the requirements disseminated in OMB Memorandum (OMB) M-20-32, *Improving Vulnerability Identification, Management, and Remediation*, published on September 2, 2020. OMB M-20-32 requires Federal agencies to implement Vulnerability Disclosure Policies that establish processes for the identification, management, and remediation of security vulnerabilities uncovered by good faith security researchers from the public. The Memorandum requires the DHS CISA to publish implementation guidance describing actions that agencies should take to implement VDP.

On September 2, 2020, the DHS published Binding Operational Directive (BOD) 20-01, *Develop and Publish a Vulnerability Disclosure Policy*. The BOD details requirements for Government agencies to develop and publish a VDP and a supporting Vulnerability Disclosure Handling Procedures document. It requires agencies to achieve specific milestones within set dates after the publishing of the BOD, including publishing a VDP on a public web page within 180 days of the BOD's issuance date and expanding the system scope of the VDP by at least one system within 270 days after the BOD's issuance date. The corresponding FISMA Reporting Metric measures agency compliance with OMB M-20-32 and BOD 20-01.

OVERVIEW OF THE FDIC'S INFORMATION SECURITY PROGRAM

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

The FDIC Chairman has delegated the authority to ensure compliance with FISMA to the FDIC's CIO. The CIO reports directly to the FDIC Chairman and has broad strategic responsibility for IT governance, investments, program management, and information security. The CIO also serves as the Chief Privacy Officer (CPO)[11] and the Director of the Division of Information Technology (DIT). As the CPO, which is a statutorily mandated position, the CIO serves as the Senior Agency Official for Privacy (SAOP)

[11] 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 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 security professionals within the Office of the CISO (OCISO), which is part of the CIO 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 within the FDIC appoints an Information Security Manager (ISM) responsible for applying the agency-wide approach to information security. The ISMs are responsible for assessing security and the level of risk in applications utilized within their division, identifying and classifying major applications, and ensuring that information security requirements are properly addressed in all new and modified systems. ISMs also act as a liaison between regional and field offices, corporate management, and DIT security personnel. Additionally, ISMs ensure that employees and contractors are aware of corporate-wide security and privacy requirements.

CIOO Reorganization

On September 27, 2020, the FDIC reorganized its CIOO in an effort to align with the activities within the Systems Development Lifecycle framework:

- Planning
- Analysis
- Design
- Development
- Testing
- Implementation
- Operations and Maintenance

In addition to reorganizing existing roles, the effort also established new senior leadership roles:

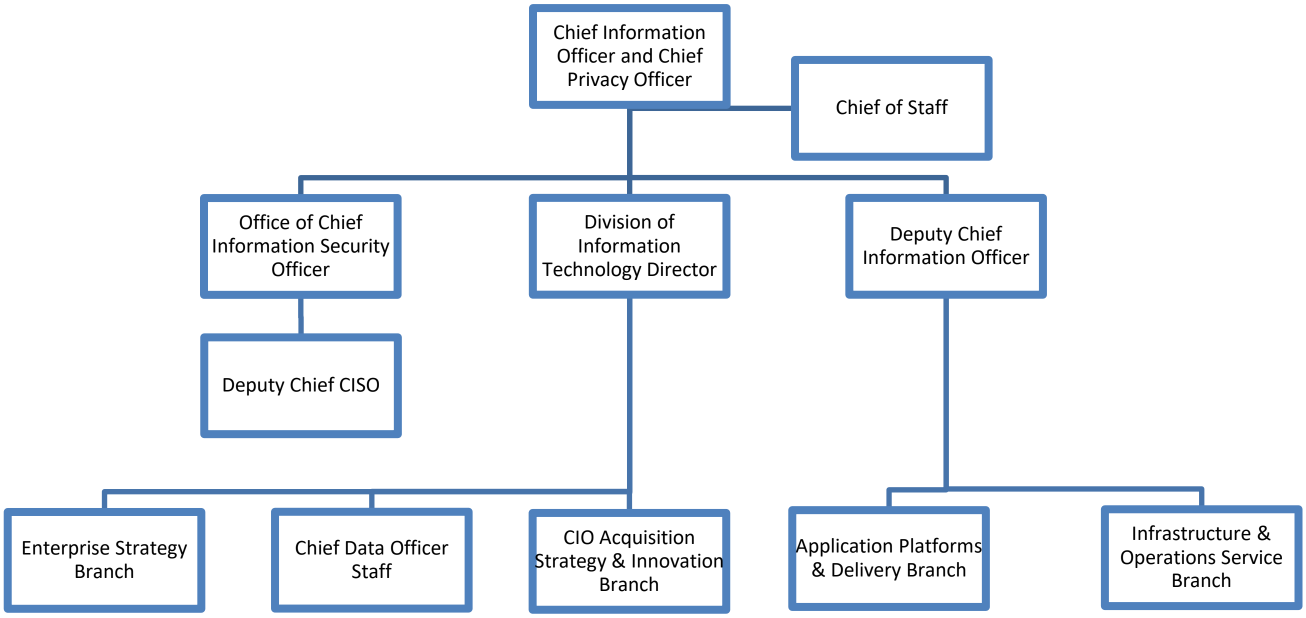
- The Deputy CIO (DCIO) reports to the CIO and provides strategic leadership, oversight, and management direction/guidance to members of the CIOO's Senior Leadership Team. The DCIO's responsibilities include managing end-to-end CIOO financial and management services and ensuring that the FDIC successfully migrates towards a working DevSecOps[12] model.

[12] DevOps is an emerging set of software development and management practices that combines the development and operations teams into a single team. DevSecOps is the philosophy of integrating security practices within the DevOps process.

- The Chief Data Officer (CDO) and supporting staff work to align the data-related functions across the organization and address a vision for data management.

Below is a visual representation of the reorganized CIO Organization:

Figure 2: CIO Organization Chart


Chief Information Officer and Chief Privacy Officer
Chief of Staff
Office of Chief Information Security Officer
Division of Information Technology Director
Deputy Chief Information Officer
Deputy Chief CISO
Enterprise Strategy Branch
Chief Data Officer Staff
CIO Acquisition Strategy & Innovation Branch
Application Platforms & Delivery Branch
Infrastructure & Operations Service Branch

Source: FDIC Intranet.

Additionally, on March 1, 2021, FDIC reorganized the OCISO – an office under the CIOO - into five distinct sections.

- Mission Integration Section, which leads OCISO program management and planning to integrate and coordinate across OCISO, CIOO, and the FDIC.
- Cyber Assurance Services Section, which performs Information Systems Security Engineer and Enterprise Security Architecture functions.
- Cyber Risk Management Section, which provides oversight of the FDIC's Risk Management Framework (RMF) implementation, including the Assessment and Authorization process.
- Enterprise Security Operations Section, which defends the enterprise from cybersecurity incidents and threats.
- Privacy Program Section, which manages privacy risk through a Privacy Continuous Monitoring program, and promotes a privacy-positive ecosystem by informing the use of technologies, —

such as artificial intelligence and machine learning; data, including data sharing, disclosure and de-identification.[13]

Summary of Results

Based on the results of our audit work and the application of the DHS FISMA Reporting Metrics, we determined that the FDIC's information security program is operating at a Maturity Level 4 (*Managed and Measurable*). Achieving Level 4 does not mean that the FDIC is without risks to cyberattack. As described in our audit results, there are significant deficiencies which remain at the FDIC. Table 2 provides a breakdown of the maturity level ratings we assigned to each domain and function area, as well as the FDIC's overall information security program.

Reaching level 4 does not indicate that the FDIC's information security program is without weakness. As described in our audit results, there are significant weaknesses which remain at the FDIC. We recommend the FDIC continue to proactively address known deficiencies in the information security program, including those described below.

In addition, this numerical score should not be compared to prior or future years. The DHS FISMA Reporting Metrics undergo changes – sometimes significant – annually. The FY 2021 DHS FISMA Report Metrics suggest that significant changes are contemplated in future years. These changes, together with differences in the scope of audit work performed each year, make it imprudent to compare this year's maturity level ratings to ratings in both prior and future years.

Table 2: Maturity Level Ratings by Domain, Function Area, and the Overall Information Security Program

Function Area	Domain	Domain Rating	Function Area Rating	Overall Rating
Identify	Risk Management	3	3	4
	Supply Chain Risk Management	1*		
Protect	Configuration Management	4	4	
	Identity and Access Management	4		
	Data Protection and Privacy	3		
	Security Training	4		
Detect	ISCM	2	2	
Respond	Incident Response	4	4	
Recover	Contingency Planning	4	4	

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

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

[13] According to NIST 800-53 Rev 5, De-identification is the term for the process of removing the association between a set of identifying data and the data subject. For example, datasets may include PII. De-identification would remove the PII from the data when it is no longer necessary to satisfy the requirements envisioned for the data.

*The maturity level of the Supply Chain Risk Management Domain is not considered in the Identify Function area rating nor the overall information security program rating.

We found that the FDIC established a number of information security program controls and practices that were consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines. The FDIC also took action to strengthen its security controls following the issuance of our FISMA audit report in October 2020. For example, the FDIC:

- Continued the implementation of a Privacy Continuous Monitoring Program initiated in 2019 that integrates the implementation and assessment of privacy controls into the FDIC's RMF implementation.
- Published its first corporate-wide SCRM Program directive, defining related policy, roles, and responsibilities.
- Defined and implemented the oversight authorities, roles, and responsibilities of its Operating Committee as the FDIC's Risk Management Council.
- Created new processes to prevent unauthorized software from being installed on FDIC's network.
- Established a process to ensure that Risk Acceptance decisions are reviewed at a defined frequency.
- Enhanced its Standard Operating Procedures (SOP) and quality control processes to ensure that FDIC employees and contractors are investigated based on their roles' risk designations.
- Updated its contingency planning policies and procedures to reflect current requirements and processes, including refreshing its directive to reflect current federal contingency planning guidance; aligning recovery time objectives for mission-essential and mission-critical applications; and updating stakeholder responsibilities to reflect recent reorganizations of FDIC divisions and offices.
- Conducted a contingency plan test with unplanned emergencies and/or disruptions to simulate real-life scenarios.

Notwithstanding these actions, our report describes significant security control weaknesses that reduced the effectiveness of the FDIC's information security program and practices. The FDIC can reduce the impact to confidentiality, integrity, and availability[14] of the FDIC's information systems and risk to data by remediating these weaknesses. In some cases, these security control weaknesses were identified during separate OIG audits and evaluations, or through security and privacy control assessments completed by the FDIC. Because the FDIC had not yet completed the respective corrective actions at the time of this audit, these security control weaknesses continued to pose risk to the FDIC. A brief description of the security control weaknesses that pose the most significant risks to the

[14] NIST SP 800-12 *An Introduction to Information Security* defines information security as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability. The effectiveness of these three elements – confidentiality, integrity, and availability – determines the effectiveness of an organization's information security.

confidentiality, integrity, and availability of the FDIC's information systems and data follows. In addition, Appendix I contains the status of recommendations made in prior year FISMA audit reports.

High Number of Overdue and Unaddressed High and Moderate-Risk POA&Ms (Identify – Risk Management). NIST SP 800-53, Rev. 4, recommends that organizations implement an effective process for managing POA&Ms for their programs and information systems. In our FISMA audit report issued in 2016, we reported that the FDIC did not address security weaknesses with a risk rating of Moderate in POA&Ms for the Data Communications (DCOM)[15] general support system in a timely manner and recommended that the CIO take appropriate steps to ensure POA&Ms are addressed in a timely manner.[16] As of August 2, 2021, only 1 overdue DCOM POA&M related to the 2016 finding had not yet been remediated.

Further, in July 2021, we analyzed the entire population of open POA&Ms in the Cyber Security Assessment and Management (CSAM) system. We found that there were 176 high- and moderate-risk POA&Ms past their estimated completion date. The scheduled completion dates of these POA&Ms ranged from March 2010 to July 2021. Without consistently addressing control deficiencies timely, the FDIC will continue to face an increasing backlog of POA&Ms, leaving its data more vulnerable to security exploits from unmitigated threats and reducing its overall security posture.

FDIC's Supply Chain Risk Management Program Lacks Maturity (Identify – Supply Chain Risk Management). The FY 2021 DHS FISMA metrics introduced the Supply Chain Risk Management (SCRM) domain within the Identify function area, corresponding to the SCRM control family in NIST SP 800-53, Revision 5. Federal agencies are required to develop and implement plans and strategies to assess and monitor their supply chain risks. In addition, they are responsible for integrating supply chain risk management practices throughout the lifecycle of each system, component, service, or asset.

In June 2021, the FDIC published a corporate-wide SCRM Program directive which contains elements of an SCRM strategy. However, the FDIC has not yet defined processes and procedures that support the underlying components of the directive. For example, the FDIC has not yet documented common SCRM controls available for inheritance by FDIC information systems, including strategies for detecting and preventing counterfeit components, and details regarding acquisition tools and techniques to protect its supply chain. Without these SCRM processes and procedures, the FDIC cannot be assured that it will accurately identify and monitor its supply chain risks. The FDIC cannot be sure that its products, system components, systems, and services provided by external parties are maintained consistently with its cybersecurity requirements, thus placing it at increased risk of exploitation through its supply chain.

Administrative Account Management Needs Improvement (Protect – Identity and Access Management). Administrative Accounts are highly sought-after targets by hackers and other adversaries who may wish to use the accounts to corrupt data, launch attacks, or conduct other malicious activities. As a result, Administrative Accounts must be carefully provisioned, monitored, and deactivated when no longer necessary.

We have reported weaknesses related to Administrative Account management in each of our past four FISMA audit reports issued since 2017. Our FY 2020 FISMA report found that as of August 26, 2020,

[15] DCOM is the FDIC communications infrastructure that provides connectivity among computing services among the FDIC's data centers.

[16] This recommendation is listed in Appendix I as Recommendation 5 from the FISMA audit report issued in 2016.

there were 14 open POA&Ms in CSAM that related to weaknesses in the FDIC's management of Administrative Accounts. The report included a recommendation to implement control improvements for the management of Administrative Accounts. As of September 2021, this recommendation remained unimplemented as 3 of the 14 POA&Ms remained open. Further, during FY 2021, we identified 10 additional open POA&Ms related to privileged user access.

Weaknesses in the FDIC's processes for managing Administrative Accounts increased the risk of unauthorized activity, such as individuals accessing, modifying, deleting, or exfiltrating sensitive information. In light of repeated weaknesses in this area, the FDIC should take steps to identify the underlying causes of the Administrative Account management weaknesses and take action to strengthen associated controls as we recommended in our FY2020 FISMA report.

Inadequate Oversight and Monitoring of Information Systems (Detect – ISCM). FISMA and OMB policy require Federal agencies to ensure that entities operating information systems on behalf of the Federal government meet the same security and privacy requirements as Federal agencies. Historically, several systems, components, and services that should have been assessed according to the RMF process were instead mischaracterized as subject to the now-rescinded *Outsourced Solution Assessment Methodology* (OSAM). As a result, the FDIC did not subject these systems to a proper risk assessment, authorization to operate, or ongoing monitoring in accordance with the RMF.

During the FISMA audit in 2020, OCISO staff began working with contracting officials to ensure that any new or planned contracts for outsourced systems would be subject to the RMF. However, as of June 22, 2021, according to data within the CSAM system, the FDIC had not yet completed the authorization to operate (ATO) for 10 operational systems:

- Contractor Systems
  - (b) (7)(E) [redacted]
  - 8. Anchor.fm Podcast Hosting Provider[17]
  - (b) (7)(E) [redacted]
- In-House Developed Systems
  - 10. Complete Discovery Source INC[18]

The OIG also identified the oversight and monitoring of outsourced systems as a weakness in its Top Management and Performance Challenges for 2020 (issued February 2021).[19] Based on the prior work from the FISMA audit, the OIG determined that "the FDIC had not properly categorized some of its

[17] Anchor.fm Podcast Hosting Provider was decommissioned during our fieldwork period. Therefore, an ATO for the system is not planned.

[18] Complete Discovery Source INC. was decommissioned during our fieldwork period. Therefore, an ATO for the system is not planned.

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

outsourced information systems, or subjected these systems to a proper risk assessment, authorization to operate, and ongoing monitoring."

OCISO officials stated that the FDIC is still migrating the legacy approvals for these systems to align with the NIST RMF as it had employed different approval processes in the past. Until the FDIC subjects all of its systems, internal or outsourced, to the RMF, the FDIC cannot be sure it will identify and address security and privacy risks in a timely manner.

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.   Due to the nature of the mode-based scoring system for the DHS Metrics, highly-rated domains still include significant risks to the FDIC IT security systems.

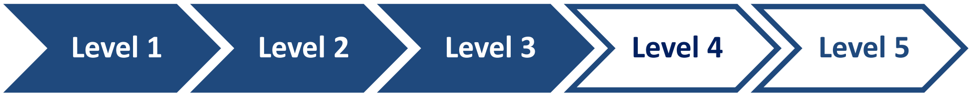
Identify

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. The NIST Cybersecurity Framework defines Risk Management as the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the potential resulting impacts. With this information, organizations can determine the acceptable level of risk for achieving their organizational objectives and can express this as their Risk Tolerance. The NIST Cybersecurity Framework states that with an understanding of Risk Tolerance, organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures.

Risk Management

The *Risk Management* domain defined in the DHS FISMA Reporting Metrics covers a wide range of activities related to 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; implementing an information security architecture; utilizing Plans of Action and Milestones (POA&M) to mitigate security weaknesses; communicating cybersecurity risks to stakeholders; and utilizing technology to provide a centralized view of cybersecurity risk management activities.

Figure 3: Maturity Rating - Risk Management



The FDIC is operating at a Maturity Level 3 (*Consistently Implemented*) in the *Risk Management* domain.

We found that the FDIC had completed a Risk Inventory and Risk Profile[20] and used an automated solution to provide a centralized view of enterprise risks, including remediation activities and risk scores. The Risk Inventory highlighted key control areas including PO&AMs and Protecting Sensitive Information. In addition, the FDIC established an information security risk management policy and supporting process and guidance documents;[21] and implemented processes for maintaining a comprehensive and accurate inventory of information systems, hardware, software, and software licenses. The FDIC had also categorized[22] and communicated the importance and priority of its systems in accordance with FISMA requirements. Further, the FDIC's IT Risk Advisory Council (ITRAC)[23] monitored IT and cybersecurity risks facing the FDIC to determine whether they were within established Risk Tolerance levels and the FDIC's Risk Appetite.

The FDIC also completed corrective actions for outstanding audit recommendations from the OIG's evaluation report entitled *The FDIC's Implementation of Enterprise Risk Management* (ERM Report) related to undefined ERM Governance, Roles, and Responsibilities noted in our 2020 FISMA Report. In addition, the FDIC completed corrective actions for a recommendation issued in our 2020 FISMA Report related to the FDIC's inconsistent re-validation of its prior risk acceptance decisions. The OIG closed these corresponding recommendations.

Notwithstanding the score in the FDIC's Risk Management domain, we have concerns about risk management at the FDIC, particularly because the FDIC did not address that many POA&Ms that were considered to be high- and moderate-risk areas.

High Number of Overdue and Unaddressed POA&Ms

NIST SP 800-53, Rev. 4, recommends that organizations implement an effective process for managing POA&Ms for their programs and information systems. In our FISMA audit report issued in 2016, we reported that the FDIC did not address security weaknesses with a risk rating of Moderate in POA&Ms for the Data Communications (DCOM) [24] general support system in a timely manner. In 2016, we recommended that the CIO review its then-existing resource commitments and priorities for addressing POA&Ms related to DCOM, and take appropriate steps to ensure POA&Ms are addressed in a timely manner.[25] In its Top Management and Performance Challenges report for 2020, the OIG identified timely corrective actions for this finding in its Top Management and Performance Challenges report for 2020.[26]

[20] The FDIC defines a *Risk Profile* as a prioritized list of the most significant risks identified and assessed through the risk assessment process.

[21] FDIC Directive 1310.3, *Information Security Risk Management Program* (March 2020), and various process and guidance documents developed by the CIOO including, but not limited to the: *Information Security Risk Management Guide: Systems and Applications* (July 2018); *InfoSec Risk Prioritization Guidelines* (January 2020); *FDIC System Prioritized Impact Level & InfoSec Risk Summary Methodology* (January 2020); and *FDIC System Security Authorization Process Guide* (June 2020).

[22] NIST FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004), requires agencies to categorize their information systems as high, moderate, or low. This category reflects the potential impact to the agency should certain events occur that jeopardize the information and information systems needed to accomplish the agency's assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

[23] The ITRAC is comprised of the CIO, CISO, Chief Risk Officer, and other FDIC stakeholders.

[24] According to the DCOM description on CSAM, DCOM is the FDIC communications infrastructure that provides connectivity among computing services among the FDIC data centers.

[25] This recommendation is listed in Appendix I as Recommendation 5 from the FISMA audit report issued in 2016.

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

In May 2020, the CIOO established a project team to work with subject matter experts to resolve open POA&Ms related to DCOM and expected to address our prior recommendation by June 2021. As of August 2, 2021, 1 overdue DCOM POA&M related to the finding had not yet been remediated.

Further, in July 2021, we analyzed the entire population of open POA&Ms in the CSAM system. We found that there were 176 high- and moderate-risk POA&Ms past their estimated completion dates. The scheduled completion dates of these POA&Ms range from March 2010 to July 2021. Specifically:

- 1 has a scheduled completion date in 2010;
- 1 has a scheduled completion date in 2013;
- 2 have a scheduled completion date in 2016;
- 1 has a scheduled completion date in 2018;
- 44 have a scheduled completion date in 2019;
- 69 have a scheduled completion date in 2020;
- 58 have a scheduled completion date in 2021.

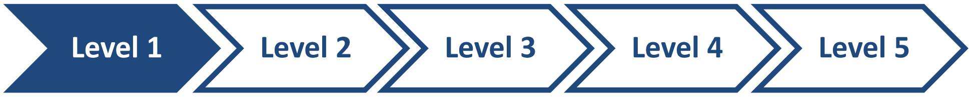
In July 2021, nearly 5 years after our previous recommendation in 2016, the FDIC's Information Operations Services Branch (IOSB) developed a POA&M Management Plan to address the earlier recommendation and to resolve its growing backlog of POA&Ms, leveraging SAFe[27] and lean agile principles to reduce the backlog.

Nevertheless, without consistently addressing control deficiencies timely, the FDIC will continue to face an increasing backlog of POA&Ms, leaving its data more vulnerable security exploits from unmitigated threats and reducing its overall security posture.

Supply Chain Risk Management

The newly added *Supply Chain Risk Management* domain defined in the DHS FISMA Reporting Metrics covers a wide 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; ensuring that external providers are operating in accordance with the FDIC's cybersecurity and supply chain requirements; and ensuring the authenticity of the components supporting FDIC systems.

Figure 4: Maturity Rating – Supply Chain Risk Management



The FDIC is operating at a Maturity Level 1 (*Ad hoc*) in the *Supply Chain Risk Management* domain.

[27] The Scaled agile framework (SAFe) is a set of organization and workflow patters intended to guide enterprises in scaling lean and agile practices, promoting alignment, collaboration, and delivery across large numbers of teams.

In November 2019, the FDIC initiated the Supply Chain Risk Management Implementation Project (SCRM Project) to build a supply chain risk-aware culture and establish an SCRM framework and governance structure. On June 24, 2021 the FDIC issued its Directive 3720.01, *Supply Chain Risk Management (SCRM) Program*, which is based on applicable NIST standards and guidelines and is consistent with FISMA requirements. Specifically, the FDIC communicated a policy that identified items to implement, including a risk appetite and tolerance; strategy and controls; evaluating and monitoring supply chain risks; an approach for implementing and communicating the strategy; and associated roles and responsibilities.

The OIG has identified the management of supply chain risk as a challenge for the FDIC in its Top Management and Performance Challenges reports for the past three years, dating back to 2018.[28] As noted in the recent OIG Top Challenges document, the GAO, NIST, and OMB have all provided guidance on Supply Chain risks over the past several years since at least 2015, and have updated their guidance over time.

However, the FDIC's SCRM Program is still in its initial phase and procedures that support the underlying components have not yet been defined in accordance with FISMA requirements. The FDIC did not have procedures that defined:

- How to implement its SCRM policy or strategy and associated baseline SCRM controls;
- Obtaining assurance over external service providers' compliance with the FDIC's SCRM requirements, including:
    - How to identify and prioritize of externally provided systems, components, and services;
    - The organizational requirements for cybersecurity and SCRM for externally provided systems, system components, and services;
    - The tools or methods used to validate that SCRM requirements are being met;
    - The risk-based processes for evaluating SCRM risks associated with suppliers;
    - How awareness is maintained over risks stemming from upstream suppliers through monitoring activities; and
    - The integration of its acquisition process and the use of contractual stipulations detailing appropriate SCRM measures for external providers;
- Management of counterfeit components, including:
    - How to detect and prevent counterfeit components;
    - How to maintain configuration control over components being repaired or serviced;
    - The process for reporting counterfeit components.

According to FDIC Directive 3720.01, *Supply Chain Risk Management Program*, the FDIC depends on a variety of products, systems, and services from external providers to fulfill its mission. Because the FDIC is a financial regulator and holds sensitive and nonpublic information, it is a potential target of adversaries seeking to interfere with its regulatory activities or obtain information for their own advantage. Immature SCRM processes limit the FDIC's ability to identify vulnerabilities throughout its supply chain consistently, and to manage and monitor associated risks effectively.

[28] Under the Reports Consolidation Act of 2000, the Office of Inspector General (OIG) annually identifies the Top Management and Performance Challenges (TMPC) facing the FDIC.

Recommendation

We recommend that the Chief Risk Officer:

1. Develop and implement SCRM processes and procedures in accordance with the Supply Chain Risk Management Program Directive and applicable government guidance.

PROTECT

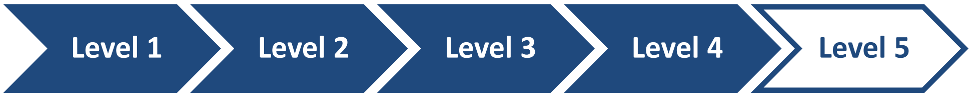
The objective of the *Protect* function is to develop and implement safeguards to secure information systems. The *Protect* function supports the ability to prevent, limit, or contain the impact of a cybersecurity event through configuration management, identity and access management, data protection and privacy, and security training.

Configuration Management

Ensuring the integrity, security, and reliability of any information system requires 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. Managing these types of changes is referred to as configuration management. Organizations help to ensure the integrity of IT products and systems by implementing processes for initializing, changing, and monitoring their configuration throughout the system development life cycle.

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.

Figure 5: Maturity Rating - Configuration Management



The FDIC is operating at a Maturity Level 4 (*Measured and Manageable*) in the *Configuration Management* domain.

The FDIC established a number of configuration management controls that were consistent with FISMA requirements and applicable NIST standards and guidelines. For example, the FDIC established configuration management policies;[29] an Infrastructure Change Control Board to review and approve changes to the IT infrastructure; and a centralized system to track, manage, and report software configuration changes. The FDIC also completed actions to address a recommendation made in the FY 2020 FISMA audit report related to preventing the unauthorized installation of software on the FDIC network.[30]

However, the FDIC had not completed work to develop or update baseline configurations for certain network IT devices as previously recommended in our FY 2020 FISMA Report. Further, the FDIC had an open POA&M as of August 2, 2021 stating that one system's traffic is not routed through a Trusted Internet Connection.

Incomplete Baseline Configurations for Certain IT Systems

FISMA requires Federal agencies to ensure compliance with minimally acceptable system configuration requirements, as determined by the agency. Organizations establish configuration requirements for their information systems in a document or repository called a "baseline configuration." A baseline configuration defines the required specifications for a system, such as its required security settings, software version, patch levels, and documentation. Baseline configurations must be approved by the Change Control Board and changed only through a formal change control process. Organizations use baseline configurations as a frame of reference to assess their systems for compliance with configuration requirements and to help manage future builds, releases, and/or changes[31]. Baseline configurations, therefore, serve as an important control for securing and managing changes to information systems.

The FDIC had established and implemented baseline configurations for primary components of its operating systems. However, as of July 21, 2020, the FDIC had 13 open POA&Ms related to incomplete or out-of-date baseline configurations. The POA&Ms addressed certain key network IT devices, including (b) (7)(E). Notably, the estimated completion dates for 5 of the 13 POA&Ms were past due, and 3 were more than 200 days past due. We issued a recommendation in our FY 2020 report to remediate these incomplete and outdated baseline configurations.

As of August 2, 2021, this prior year recommendation remained open. The FDIC estimates it will complete corrective actions for this finding by February 28, 2022. Without complete baseline configurations for these IT devices, the FDIC cannot be sure that it will identify and remediate known vulnerabilities or misconfigurations in a timely manner. This increases the FDIC's susceptibility to attacks where its baselines are not configured in accordance with recommended hardening guidelines.[32]

[29] Such policies included FDIC Directive 1320.4, *FDIC Software Configuration Management Policy* (January 2017); CIOO Policy No. 18-004, *IT Infrastructure and Security Change Management* (July 2018); CIOO Policy No. 19-005, *Policy on Security Patch Management* (April 2019); and CIOO Policy No. 16-005, *Policy on Secure Baseline Configuration Guides* (December 2016).

[30] This recommendation is listed in Appendix I as Recommendation 2 from the FISMA audit report issued in 2020.

[31] Builds, releases, and changes are elements of the software development life cycle. A build is typically a version of software in pre-release format. A change typically modifies features of applications or systems to suit different requirements, patches, or upgrades.

[32] NIST SP 800-123, *Guide to General Server Security* defines Hardening as configuring a host's operating system and applications to reduce the host's security weaknesses.

Trusted Internet Connection Initiative Not Fully Implemented

In November 2007, OMB announced the Trusted Internet Connections (TIC) initiative.[33] The TIC initiative initially focused on making agency network connections "trusted" by (a) reducing the number of external network connections used by executive branch agencies and (b) deploying common security tools at these connection points to more effectively monitor incoming and outgoing network traffic for potentially malicious activity. By implementing OMB's TIC initiative, agency network connections may become "trusted." In the years following OMB's announcement of the TIC initiative, OMB issued additional guidance and updates.[34]

The FDIC's Legal Division determined that OMB Memorandum M-08-05 and subsequent guidance and updates on the TIC initiative were not legally binding on the FDIC. As a result, the FDIC did not initially implement OMB's TIC initiative.

However, in September 2019, OMB issued Memorandum OMB M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative*, which rescinded OMB Memorandum M-08-05 and OMB's prior guidance and updates on the TIC initiative. OMB M-19-26 provided Federal agencies with new guidance on what had become the third iteration of the TIC initiative (referred to hereinafter as TIC 3.0). In October 2019, the FDIC's Legal Division reversed its previous position concerning the TIC initiative and determined that OMB M-19-26 is binding on the FDIC, because this memorandum is grounded in the statutory authority of FISMA.[35]

OMB M-19-26 defines an enhanced approach for implementing TIC 3.0 and requires agency CIOs to maintain an accurate inventory of their agency network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection. According to OMB M-19-26, agencies must maintain such information in case it is needed "to assist with government-wide cybersecurity incident response or other cybersecurity matters." In addition, OMB M-19-26 required agencies to update their network and system boundary policies, and identify appropriate TIC Use Cases[36] by September 12, 2020.

At the close of our audit field work for last year's FISMA report in September 2020, the FDIC had taken action to address the requirements of TIC 3.0, as it had identified its external network connections and developed TIC Use Cases. The FDIC also deployed physical sensors to implement the security capabilities outlined in its TIC Use Cases.

However, as of August 2, 2021, the FDIC had identified an instance of its traffic not routing through a defined TIC access point per FISMA requirements for one system. The CIOO intends to enable and

[33] OMB Memorandum M-08-05, *Implementation of Trusted Internet Connections (TIC)* (November 2007).
[34] OMB Memoranda: M-08-16, *Guidance for TIC Statement of Capability Form (SOC)* (April 2008); M-08-27, *Guidance for TIC Compliance* (September 2008); and M-09-32, *Update on the TIC Initiative* (September 2009).
[35] OMB Memorandum M-19-26, *Update to the TIC Initiative* (September 2019), states that OMB and DHS will track implementation of the TIC program through FISMA reporting (page 3).
[36] DHS is responsible for defining TIC initiative requirements in documentation called TIC Use Cases. TIC Use Cases outline which alternative security controls, such as endpoint and user-based protections, must be in place for specific scenarios in which traffic may not be required to flow through a physical TIC access point.

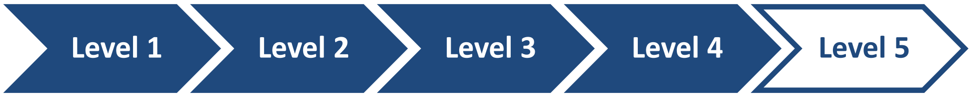
enforce multifactor authentication for external users connecting to the system consistent with the interim guidance for the TIC 3.0 Remote User Use Case.[37] Implementation began on August 30, 2021.

Identity and Access Management

Identity and Access Management involves 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 an Identity, Credential, and Access Management (ICAM) strategy, policies, procedures, and a roadmap that addresses Federal guidance.[38] Identity and Access Management also involves performing personnel screening (including background investigations), issuing and maintaining user credentials (usernames and passwords), executing non-disclosure and confidentiality agreements, and managing logical and physical access privileges.

FISMA requires agency information security programs to include risk-based policies and procedures that address unauthorized access to, and use of, information and information systems. In addition, NIST SP 800-63, *Digital Identity Guidelines* (June 2017) provides guidance for establishing and implementing appropriate identification and authentication controls and access controls for Federal information and information systems. In addition, Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, mandates a government-wide standard for secure and reliable forms of identification issued by departments and agencies for employees and contractors.

Figure 6: Maturity Rating – Identity and Access Management



The FDIC is operating at a Maturity Level 4 (*Managed and Measurable*) in the *Identity and Access Management* domain.

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,[39] and policies and procedures for identifying, authenticating, and managing users who access FDIC information systems and facilities.[40] In addition, the FDIC updated its procedures and processes to ensure that its employees and contractors are appropriately investigated based on their job functions' risk designations.

[37] The Cybersecurity and Infrastructure Security Agency (CISA) released a draft version of its use case for remote users in December 2020. Finalized guidance has not yet been released.

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

[39] 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.

[40] 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).

However, the FDIC's administrative account management needed improvement and the FDIC did not always maintain Confidentiality Agreements for its contractor personnel as required by FDIC policy.

Administrative Account Management Needs Improvement

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

Our FY 2020 FISMA report found that as of August 26, 2020, there were 14 open POA&Ms in CSAM that related to weaknesses in the FDIC's management of Administrative Accounts. These weaknesses included (b) (7)(E) [redacted]. Our FY 2020 FISMA report included a recommendation to implement control improvements for the management of Administrative Accounts. As of August 31, 2021, this recommendation remained unimplemented. Specifically, three of the 14 POA&Ms from the prior year remained open. Additionally, during FY 2021, we identified 11 additional open POA&Ms related to (b) (7)(E) [redacted]. The FDIC estimates that it will implement Administrative Account control improvements by December 30, 2021.

In addition to the deficiencies identified above, we have reported similar weaknesses related to Administrative Account management in each of our past four FISMA audit reports issued since 2017. Additionally, in May 2019, the FDIC OIG reported, in its report on Cyber Threats, that the FDIC did not always require firewall administrators to uniquely identify and authenticate when accessing network firewalls.[41] The OIG also noted in its report that some (b) (7)(E) [redacted], which is prohibited by FDIC policy.

Further, in November 2018, a consulting firm engaged by the FDIC to assess the effectiveness of the internal network security controls[42] identified more than 1,500 instances in which: (b) (7)(E) [redacted]. The consulting firm recommended resetting weak passwords and potentially implementing (b) (7)(E) [redacted] to remediate these weaknesses.

Weaknesses in the FDIC's processes for managing Administrative Accounts increased the risk of unauthorized activity, such as individuals accessing, modifying, deleting, or exfiltrating sensitive information. In light of repeated weaknesses in this area, the FDIC should take steps to identify the underlying causes of the Administrative Account management weaknesses and take action to strengthen associated controls as we recommended in our FY2020 FISMA report.

[41] FDIC OIG Report, *Preventing and Detecting Cyber Threats* (Report No. AUD-19-005, May 2019), https://www.fdicoig.gov/sites/default/files/publications/19-005AUD.pdf. The report contained 10 recommendations
[42] FDIC Internal Adversary Simulation Security Assessment Report, prepared for the FDIC on January 24, 2019.

Contractor Confidentiality Agreements Not Consistently Maintained

The FDIC's Acquisition Policy Manual (APM)[43] states that if a contractor, its personnel, or its subcontractors may have access to FDIC facilities or systems, or otherwise may have access to FDIC sensitive information, such contractor personnel shall sign a Confidentiality Agreement[44] prior to receiving or collecting sensitive FDIC information. Confidentiality Agreements inform contractor personnel of their obligations regarding the proper handling and safeguarding of sensitive information, and hold individuals accountable who fail to meet those obligations. The APM states that contracting personnel shall maintain Confidentiality Agreements in the official contract file.

The FDIC did not maintain signed Confidentiality Agreements for contractor and subcontractor personnel working on a key facilities management contract[45]. Both the APM and the terms of the facilities management contract required the contractor and subcontractor personnel to sign a Confidentiality Agreement, because these personnel had access to the FDIC's network and/or sensitive areas of FDIC facilities. After these exceptions were brought to the attention of the FDIC, the Oversight Manager for the facilities management contract requested the contractor and subcontractor personnel to sign a Confidentiality Agreement.

As of August 2, 2021, one of three recommendations related to signed Confidentiality Agreements remains unimplemented. The FDIC estimates it will complete the remaining corrective action for the final recommendation by December 31, 2021.

The lack of signed Confidentiality Agreements for the facilities management contract was not an isolated instance. According to reports issued by the FDIC OIG, the FDIC did not consistently execute or maintain Confidentiality Agreements for its contractor personnel that handled sensitive information, such as bank data and PII, or that provided critical services, such IT and security services in support of bank closings. For example, in September 2017, the OIG reported that the FDIC could not locate signed confidentiality agreements for 36 of the 48 contractor personnel.[46] In October 2012, the OIG reported that the FDIC did not consistently execute and maintain Confidentiality Agreements for contractor and subcontractor personnel.[47] In September 2008, the OIG reported that the FDIC did not maintain Confidentiality Agreements for 14 of 46 contractor personnel reviewed.[48] In January 2006, the OIG reported that the FDIC did not maintain signed Confidentiality Agreements for 12 of 13 contracts reviewed.[49]

Without signed Confidentiality Agreements, it is difficult for the FDIC to pursue administrative, civil, or criminal actions against contractor personnel who fail to properly handle or safeguard sensitive FDIC information and assets. Further, the FDIC has reduced assurance that contractor personnel will understand their responsibilities for protecting the confidentiality, integrity, and availability of sensitive

[43] FDIC Directive 3700.16, FDIC Acquisition Policy Manual (APM).

[44] FDIC Form 3700/46A, *Confidentiality Agreement*.

[45] FDIC OIG Report, *Security of Critical Building Services at FDIC-owned Facilities* (Report No. AUD-21-003, March 2021).

[46] FDIC OIG Report, *Controls over Separating Personnel's Access to Sensitive Information* (Report No. EVAL-17-007, September 2017), https://www.fdicoig.gov/sites/default/files/publications/17-007EV_0.pdf.

[47] FDIC OIG Report, *Invoices Submitted by Lockheed Martin Services, Inc. under the FDIC's Data Management Services Contract* (Report No. AUD-13-002, October 2012), https://www.fdicoig.gov/sites/default/files/publications/13-002AUD.pdf.

[48] FDIC OIG Report, *Protection of Resolution and Receivership Data Managed or Maintained by an FDIC* Contractor (Report No. AUD-08-015, September 2008), https://www.fdicoig.gov/sites/default/files/publications/08-015.pdf.

[49] FDIC OIG Report, *FDIC Safeguards Over Personal Employee Information* (Report No. EVAL-06-005, January 2006).

information. Absent signed Confidentiality Agreements, the FDIC is at increased the risk of an unauthorized disclosure of sensitive information.

The FDIC Has Not Begun Tracking Progress on Updated ICAM Roadmap Milestones

OMB Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management,* states that each agency shall define and maintain a single comprehensive ICAM policy, process, and technology solution roadmap. These items should encompass the agency's entire enterprise; align with the Government-wide Federal Identity, Credential, and Access Management (FICAM) Architecture and Continuous Diagnostics and Mitigation (CDM) requirements; incorporate applicable Federal policies, standards, playbooks, and guidelines; and include roles and responsibilities for all users.

The FDIC had developed an ICAM Strategy and ICAM Roadmap that documented its approach and planned initiatives for identifying, credentialing, monitoring, and managing access to its resources by the end of 2019. However, the ICAM team determined the 2019 ICAM Roadmap to be inadequate as many of its initiatives needed to be re-prioritized. We further learned that there was no documented evidence that the 2019 ICAM Roadmap had received approval from the ICAM steering committee. Therefore, at the beginning of 2021, the FDIC ICAM Program put all existing initiatives on hold as it reevaluated its roadmap and performed an internal assessment of its overall ICAM Program. The FDIC used this assessment to create an updated five-year ICAM Roadmap that will begin in FY 2022. Since the FDIC is creating a new ICAM Roadmap, it is not actively tracking the completion progress of the 2019 ICAM initiatives. The ICAM Roadmap includes significant identity and access management initiatives, such as the development of a Centralized Authentication Hub to centrally manage all user access permissions and authentication requests across multiple external applications and moving Access Management to the Cloud. If the FDIC does not track its revised ICAM Roadmap milestones, the FDIC is at risk that it will not achieve its identity and access management objectives in a timely manner, leaving its infrastructure and applications vulnerable to unauthorized access.

Recommendations

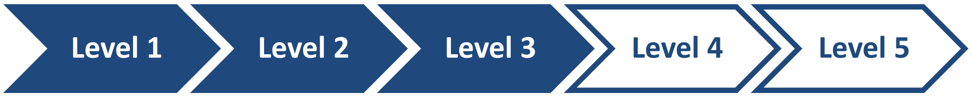
We recommend that the CIO:

2. Begin tracking completion of ICAM milestones of its revised ICAM Roadmap.

Data Protection and Privacy

Data Protection and Privacy involves implementing a privacy program to properly collect, use, maintain, 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, minimizing PII holdings, and breach response planning.

Figure 7: Maturity Rating – Data Protection and Privacy



The FDIC is operating at a Maturity Level 3 (*Consistently Implemented*) in the *Data Protection and Privacy* domain.

OMB Circular A-130 requires Federal agencies to establish and maintain a comprehensive privacy program that ensures compliance with applicable privacy requirements. OMB Circular A-130 requires agencies to:

- Reduce their PII holdings to the minimum amount necessary for the proper performance of authorized agency functions;
- Conduct privacy impact assessments, as prescribed by the E-Government Act of 2002,[50] when the agency develops, procures, or uses IT to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII;
- Implement the Risk Management Framework (RMF)[51] in NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations*, when categorizing information systems; selecting, implementing, and assessing controls; authorizing systems to operate; and monitoring controls; and
- Establish and maintain an agency-wide Privacy Continuous Monitoring (PCM) strategy and PCM program.[52]

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 a Privacy Program Policy,[53] Privacy Program Plan, and Breach Response Plan. The FDIC also tests its Breach Response Plan annually and employs mechanisms, such as firewalls, email authentication technology, and Data Loss Prevention (DLP) tools, to detect and minimize exfiltration of information.

Additionally, the FDIC issued a Document Labeling Directive that establishes requirements for categorizing and labeling documents. However, the FDIC had not yet completed action to address a recommendation included in our FISMA audit report issued in 2019 aimed at monitoring employee and contractor compliance with requirements for safeguarding sensitive electronic and hardcopy information, including PII.

Additionally, although the FDIC made substantial progress in improving its Privacy Program and establishing processes to close a majority of the recommendations from the OIG's audit of the FDIC's Privacy Program, completed in December 2019, it was still implementing those processes across the entire organization during our audit fieldwork.

[50] Section 208 of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (codified at 44 U.S.C. § 3501 note) requires agencies to conduct Privacy Impact Assessments of IT and collections of information and make them available to the public. A Privacy Impact Assessment is a process for examining the risks of using IT to collect, maintain, and disseminate PII from or about members of the public.

[51] The RMF defines a disciplined and structured process that integrates information security, privacy, and risk management activities into the information system development lifecycle.

[52] The purpose of the PCM strategy is to identify the privacy controls implemented across the agency for all PII systems. The purpose of the PCM program is to verify the continued effectiveness of selected privacy controls, ensure ongoing awareness of privacy risks, and monitor changes to PII systems.

[53] FDIC Directive 1360.20, *Privacy Program* (March 2017).

Unaddressed Privacy Control Weaknesses

Congress has enacted a number of statutes that impose privacy-related requirements on Federal agencies. In addition, OMB has issued Government-wide policies and guidance to assist agencies in fulfilling their statutory responsibilities related to privacy. Of note, in July 2016, OMB issued a revision to its Circular A-130 that updated and expanded agency requirements and responsibilities for managing PII. Appendix II of OMB Circular A-130 organizes relevant privacy-related requirements and responsibilities for Federal agencies into nine areas:

Table 3: OMB Circular A-130 Privacy requirements

Privacy Control Area	Description
General Requirements	Establish and maintain a privacy program, comply with privacy requirements, and manage privacy risks. Activities in this area include developing privacy program plans; designating an SAOP; and monitoring Federal privacy-related laws, regulations, and policies for changes.
Considerations for Managing PII	Maintain an inventory of PII; regularly review all PII held by the agency; eliminate the unnecessary collection, maintenance, and use of PII; and follow approved records retention or disposition schedules.
Budget and Acquisition	Ensure that agency privacy programs have the resources necessary to manage PII and consider privacy when acquiring or developing system technologies and services.
Contractors and Third Parties	Ensure that contractors and other third parties handling PII on behalf of the agency comply with privacy requirements. This includes incorporating privacy into agency contracts and other agreements.
Privacy Impact Assessments (PIA)	Conduct PIAs in accordance with the E-Government Act and OMB policy.
Workforce Management	Assess and address privacy hiring, training, and professional development needs.
Training and Accountability	Provide an agency-wide privacy awareness and training program for all employees and contractors and hold personnel accountable for noncompliance with privacy requirements.
Incident Response	Develop and implement incident management and response capabilities, including policies, roles and responsibilities, reporting, and periodic testing of effectiveness.
Risk Management Framework	Use the Risk Management Framework developed by NIST to manage privacy risks.

Source: OIG Privacy Team's Analysis of OMB Circular A-130, Appendix II, Report No. AUD-20-003.

As noted above, in December 2019, the OIG completed an audit that assessed the effectiveness of the FDIC's Privacy Program controls and practices in eight of the nine areas covered by Appendix II of OMB Circular A-130. According to the OIG's audit report, the FDIC's Privacy Program controls and practices were effective in four of eight areas examined. Specifically, the FDIC implemented a privacy training and awareness program; identified its privacy staffing and budgetary needs; established privacy competency requirements for key staff; and took steps to ensure contractor compliance with privacy requirements.

However, the OIG found that privacy controls and practices in the remaining four areas covered by Appendix II of OMB Circular A-130 were either partially effective or not effective, because they did not comply with all relevant privacy laws[54] and/or OMB policy and guidance. Specifically, the FDIC did not:

- Fully integrate privacy considerations into its RMF designed to categorize information systems, establish system privacy plans, and select and continuously monitor system privacy controls;
- Adequately define the responsibilities of the Deputy Chief Privacy Officer or implement Records and Information Management Unit (RIMU)[55] responsibilities for supporting the Privacy Program;
- Effectively manage or secure PII stored in network shared drives and in hard copy, or dispose of PII within established timeframes,[56] including implementing the Document Labeling initiative[57] intended to identify, categorize, label, and protect PII and sensitive information; and
- Ensure that PIAs were always completed, monitored, and retired in a timely manner.

The weaknesses identified by the OIG increased the risk of PII loss, theft, and unauthorized access or disclosure, which could lead to identity theft or other forms of consumer fraud against individuals. In addition, weaknesses related to the management of PIAs reduced transparency regarding the FDIC's practices for handling and protecting PII.

The OIG's audit report contained 14 recommendations. The OIG recommended that the FDIC update its policies and procedures and establish appropriate governance to ensure proper execution of privacy responsibilities; implement privacy plans for all of its systems containing PII consistent with OMB policy; and continuously monitor privacy controls. The OIG also recommended that the FDIC effectively manage and protect PII stored in network shared drives and in hard copy; complete and implement its Document Labeling initiative; implement records management requirements; and revise processes to improve the management of PIAs. As of July 29, 2021, the FDIC had taken sufficient action to close 11 of the 14 recommendations. Table 4 lists the FDIC's planned closure dates for the remaining 3 recommendations.

[54] Privacy Act of 1974, 5 U.S.C § 522a; Section 208 of the E-Government Act of 2002; Section 522 of the Consolidated Appropriations Act of 2005, amended by Consolidated Appropriations Act of 2008 (codified as amended at 42 U.S.C. § 2000ee-2).

[55] RIMU is a component office within the Division of Administration's Corporate Services Branch. RIMU provides advice and support to the Privacy Program to help ensure that records containing PII comply with the FDIC Records Retention Schedule.

[56] The Records Retention Schedule classifies all FDIC business records, including records containing PII, and prescribes approved retention periods to ensure their timely destruction at the conclusion of the established retention period.

[57] In 2016, the FDIC initiated the Document Labeling initiative (formerly known as the Data Protection Program) to establish standards, policies, support, and methods to identify, categorize, label, and protect PII and sensitive information. Until the FDIC fully implements the Document Labeling initiative, there is an increased risk that sensitive data will not be properly handled and safeguarded.

Table 4: Open Privacy Audit Recommendations

Recommendation	Planned Closure Date
Recommendation 3 Develop and approve privacy plans for all information systems containing PII consistent with OMB Circular A-130.	December 17, 2021
Recommendation 5 Update policies and/or procedures to reflect the current organizational structure of the Privacy Program and responsibilities of agency personnel and component offices that support the FDIC's Privacy Program.	December 30, 2021
Recommendation 8 Develop and implement controls to ensure that PII stored in network shared drives and in hard copy is regularly monitored and reviewed for compliance with privacy laws, regulations, policy, and guidelines.	December 17, 2021

Source: Cotton & Company LLP's analysis of planned closure dates for privacy program recommendations in the FDIC OIG's Unimplemented Recommendations Report on July 29, 2021.

Notably, the FDIC established privacy processes to close Recommendation 7: Complete and implement the data protection program policy directive, data labeling guide, and associated job aids and Recommendation 13: Revise and implement processes to ensure that PIAs are completed and made available to the public prior to authorizing information systems containing PII to operate. However, some of these processes were still being fully implemented during our audit.

Data Labeling Guide Not Fully Implemented

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

By 2021, the FDIC had begun piloting its labeling program to collect feedback for mandatory implementation. However, the FDIC does not anticipate full implementation, whereby policy enforcement will be mandatory, until 2022. Additionally, the requirements do not apply to any FDIC document created prior to the approval date of the Directive, unless the document is modified. Therefore, we did not have assurance that document labeling controls protecting the exfiltration of sensitive data were consistently implemented.

Privacy Impact Assessments Not Completed

The E-Government Act of 2002 requires Federal agencies to conduct Privacy Impact Assessments (PIAs) before developing or procuring IT that collects, maintains, or disseminates PII. It also requires agencies to make PIAs publicly available, if practicable. The OMB also issued guidance to assist agencies in implementing the privacy provisions of the E-Government Act, including provisions related to PIAs.[58] The OIG noted in its December 2019 report[59] that PIAs were not finalized for all applicable information systems. Additionally, the PIAs on the FDIC public website were outdated as nine of them related to retired systems. The OIG recommended that the CIO/CPO remediate these issues.

In response to the recommendation, the FDIC created policies and processes to ensure the appropriate management of PIAs as part of an overall PCM process, which began implementation in April 2019. However, it was still in the process of applying the policies and processes as we identified multiple legacy PIAs on the FDIC website and noted missing PIAs for 11 systems that required them. The FDIC estimated that full implementation of the PCM would take place 3 years after it began, thereby setting an approximate completion date of April 2022. Without completing all required PIAs, the FDIC may not have a complete inventory of its PII. An incomplete inventory of PII could impact the FDIC's ability help ensure the confidentiality of PII.

Unimplemented Controls Over Sensitive Information

Federal statutes, NIST security standards and guidelines, and OMB policy require agencies to safeguard sensitive information stored in electronic and hardcopy format from unauthorized access or disclosure.[60] In addition, FDIC Circular 1360.9, *Protecting Sensitive Information* (October 2015), states that only individuals who have a legitimate need to access sensitive information in the performance of their duties may be provided access. In our FISMA audit report issued in 2019, we reported that the FDIC had not adequately controlled access to sensitive hard copy information in its facilities or sensitive electronic information on its internal network shared drives.

- **Hardcopy Information.** We conducted unannounced walkthroughs of selected areas of the FDIC's Virginia Square facility in Arlington, Virginia, during our FISMA audit conducted in 2019. Our walkthroughs identified significant quantities of sensitive hardcopy information stored in unlocked filing cabinets and boxes in building hallways and other common areas. This sensitive information included confidential bank examination information, Suspicious Activity Reports, and sensitive PII, including names, Social Security Numbers, and dates of birth. This information was easily accessible to anyone in the Virginia Square facility, including to employees, visitors, and contractor personnel.
- **Electronic Information.** As part of its audit of the FDIC's Privacy Program in 2019,[61] the FDIC OIG identified instances in which sensitive electronic information stored on internal network shared drives was not properly secured. This information, which was accessible to anyone with

[58] See OMB Circular A-130 and OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

[59] FDIC OIG Report, *The FDIC's Privacy Program* (Report No. AUD-20-003, December 2019), https://www.fdicoig.gov/sites/default/files/publications/AUD-20-003.pdf

[60] The Privacy Act of 1974 states that agencies shall establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is maintained. FISMA requires agencies to provide information security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency. NIST SP 800-53, Rev. 4, and OMB Circular A-130 require agencies to restrict access to sensitive information in accordance with the security principle of "least privilege." Least privilege refers to the practice of restricting user access to those IT resources (including data) that are necessary to perform official duties.

[61] FDIC OIG Report, *The FDIC's Privacy Program* (Report No. AUD-20-003, December 2019).

access to the FDIC's internal network, included sensitive PII and information about employee performance and disciplinary actions.

We recommended in our FISMA audit report issued in 2019 that the CIO: (1) reinforce to employees and contractor personnel the importance of properly safeguarding sensitive hardcopy and electronic information, and (2) monitor employee and contractor compliance with policy requirements for properly safeguarding sensitive hardcopy and electronic information.[62] In response to the first recommendation, the FDIC issued a message in December 2019 to all employees and contractor personnel reminding them of their responsibility to protect and appropriately dispose of sensitive hard copy and electronic information, including PII. The message described actions that employees and contractor personnel should take to safeguard and dispose of sensitive information. As a result, the OIG closed the first recommendation.

In response to the second recommendation, the FDIC launched an initiative to conduct walkthroughs of its facilities nationwide to ensure information stored in common areas is secured and disposed of in a proper manner. The FDIC began conducting walkthroughs of its facilities in the Washington, D.C. metropolitan area and its Regional Offices in December 2019; however, the FDIC has temporarily placed a hold on conducting walkthroughs in light of the recent pandemic and mandatory or maximum telework of FDIC employees.

The FDIC also committed to developing a plan to monitor employee and contractor compliance with policy requirements for safeguarding sensitive electronic information on network shared drives by May 29, 2020. However, in June 2020, the FDIC extended its target date for completing a plan to December 2021. Accordingly, the second recommendation remains unimplemented.

Recommendations

We recommend that the CIO:

3. Complete implementation of the PCM process to include updating PIAs for all required systems.

4. Implement Document Labeling Guide requirements across the entire organization as dictated by business needs.

5. Perform an analysis of the feasibility of applying the Document Labeling Guide for documents that were created before the issuance of the directive.

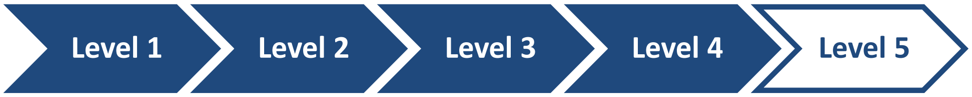
Security Training

FISMA requires agencies to provide security awareness training to their 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. In addition, FISMA recognizes that certain

[62] These recommendations are listed in Appendix I as Recommendations 1 and 2 from the FISMA audit report issued in 2019.

agency personnel have "significant security responsibilities" that require more advanced training than basic security awareness training. Advanced security training, which includes specialized and role-based security training, differs from awareness training in that it is designed to build knowledge and skills to facilitate job performance.[63]

Figure 8: Maturity Rating – Security Training



The FDIC is operating at a Maturity Level 4 (*Managed and Measurable*) in the *Security Training* domain.

FDIC Circulars 1360.16, *Mandatory Information Security Awareness Training* (March 2012) and 1360.9, *Protecting Sensitive Information* (October 2015), require all FDIC employees and contractor personnel with network access to complete security and privacy awareness training. 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 sensitive data, including PII. According to FDIC Circular 1360.16, individuals who fail to complete the awareness training requirement within 5 working days of employment, and annually thereafter, will have their access to network applications and systems revoked. This requirement was temporarily changed to 21 working days as a result of the ongoing COVID-19 pandemic.

The FDIC promotes security and privacy awareness through a variety of communication channels, such as policy documentation and dedicated security awareness webpages. On the FDICLearn webpage employees and contractor personnel can register for and complete required training courses. For example, the FDIC continued its practice of educating employees and contractor personnel about the threats associated with phishing. Phishing is a method of cyberattack in which the perpetrator sends out legitimate looking emails in an attempt to gather personal, financial, and other sensitive information from recipients, or to trick the recipients into downloading malicious software. In 2021, the FDIC updated its phishing training by adding targeted training for specialized personnel as well as a series of online and in-person follow-up training for those who are unable to successfully complete the assigned phishing exercises. The FDIC also tracks the compliance of its users and reports the data to management through the monthly ITRAC Key Risk Indicator (KRI) Metrics Reports. In these reports the monthly and quarterly compliance percentage for employees and contractor personnel enrolled in standard and specialized training courses is presented. The FDIC has set a "Green" to "Red" indicator for compliance, and as of April 2021 the FDIC has remained within its "Green" limit.

Insufficient Training on Mobile Device Security

FISMA requires Federal agencies to provide security awareness training to their 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. In addition, NIST SP 800-124, Rev. 1, *Guidelines*

[63] NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program* (October 2003), provides guidance on specialized and role-based information security training.

for Managing the Security of Mobile Devices in the Enterprise, recommends that organizations provide training and awareness to users of mobile devices on relevant threats and security practices. According to GAO, training employees on an organization's mobile security policies can help to ensure that employees use mobile devices in a secure and appropriate manner. FDIC policy requires all employees and contractor personnel with access to the FDIC's internal network to complete annual Information Security and Privacy Awareness (ISPA) Training. The FDIC requires its employees and contractors to take this training to raise their awareness of computer security and privacy laws, regulations, and policies; rules of behavior and effective security practices; and compliance requirements governing the FDIC's collection, use, sharing, and protection of sensitive data, including PII.

However, a previous audit of Mobile Device Security and Management[64] found that the ISPA Training contained limited information on threats to mobile devices and security practices for mitigating those threats. This occurred because the FDIC based its ISPA Training on FDIC Circulars 1300.4, *Acceptable Use Policy for IT Resources* (October 2018), and 1360.9, *Protecting Sensitive Information* (October 2015), which contain limited content on mobile device threats and security practices. The ISPA Training did not address the following areas (several of which are covered in the FDIC's IT policies):

- Risks associated with using unsecured public Wi-Fi hotspots, and guidance on how to identify and connect to secure wireless networks when users must access public hotspots.
- Guidance for identifying suspicious activity on mobile devices, such as blocked attempts to access the secure container and text messages from unknown parties that include links to potentially malicious websites.
- Risks associated with downloading mobile applications, such as privacy concerns associated with applications that can track user activities.
- Security considerations regarding the use of Bluetooth to connect mobile devices with peripheral devices.
- Risks associated with texting sensitive FDIC information to other individuals.
- Security precautions users should take prior to, during, and immediately following, foreign travel.

The OCISO concurred with the recommendation issued in this area and intends to update its information security and privacy awareness training by February 28, 2022.

The FDIC OIG identified other issues in this domain in its report to Critical Building Services, related to contractors and subcontractors who did not complete required Information Security and Privacy Awareness Training and Insider Threat and Counterintelligence Awareness Training. The OIG recommended that the FDIC include a provision in its future contracts requiring contractor and subcontractor personnel to complete requisite training. The FDIC concurred the recommendations and plans to complete corrective actions by December 31, 2021.[65]

[64] FDIC OIG Report, *Security and Management of Mobile Devices*, AUD-21-004, August 2021, https://www.fdicoig.gov/sites/default/files/publications/AUD-21-004.pdf.

[65] FDIC OIG Report, *Security of Critical Building Services at FDIC owned Facilities*, AUD-21-003, March 2021, fdicoig.gov/sites/default/files/publications/AUD_21_003_Redacted.pdf

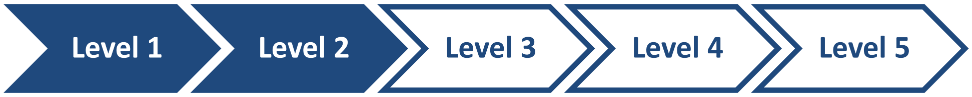
DETECT

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

Information Security Continuous Monitoring

OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems* (November 2013), requires Federal agencies to continuously monitor their information system security controls and the environments in which the systems operate. NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (September 2011), defines an organization-wide approach to continuous monitoring that supports risk-based decision making at the organization, mission/business process, and information systems tiers. NIST defines continuous monitoring as the process of maintaining an ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. An effective continuous monitoring program provides timely information and insights into security control effectiveness for senior leaders to make ongoing risk-based decisions affecting their mission and business functions.

Figure 9: Maturity Rating – Information Security Continuous Monitoring



The FDIC is operating at a Maturity Level 2 (*Defined*) in the *Information Security Continuous Monitoring* domain.

The FDIC established and implemented policies and guidance to support the continuous monitoring of its information systems.[66] In addition, the CISO implemented a System Security Authorization Process Guide to assist all FDIC stakeholders who are responsible for ensuring or managing information system security and privacy risks in accordance with the NIST RMF. The FDIC follows steps identified from the guidance to authorize information systems with an ATO decision letter before placing systems into production. 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.

However, we found that the FDIC did not consistently authorize 10 in-house and contractor owned information systems that currently process FDIC information and data. Further, the FDIC had not yet remediated a recommendation from our FY 2020 FISMA report regarding implementing a process to

[66] FDIC Directive 1310.3, *Information Security Risk Management Program* (March 2020), and the *Information Security Risk Management Guide: Systems and Applications* (July 2018).

ensure that all outsourced information systems are subject to the NIST Risk Management Framework as prescribed by OMB policy.

Cloud-based Systems Not Subject to Annual Control Assessments

FISMA requires Federal agencies to test and evaluate the effectiveness of their information system security controls at least annually. The *FDIC Security and Privacy Control Assessment (SCA) Methodology* requires the FDIC to assess the security and privacy controls for its cloud-based information systems every 3 years, with some controls required to be tested every year. In the FY 2020 FISMA audit, we reviewed the status of the FDIC's security and privacy control assessments for all 14 cloud-based systems that the FDIC had authorized to operate as of April 1, 2020. These 14 systems provided critical IT services, such as email, IT helpdesk ticketing, and hosting of the FDIC's public web site. We found that the CIOO did not subject these 14 systems to annual security and privacy control assessments in accordance with FISMA and subsequently issued a recommendation. Additionally, in two cases, the FDIC had not completed annual control assessments for more than 3 years after the FDIC authorized the systems to operate in accordance with the FDIC's methodology.

In September 2019, the FDIC created a POA&M to remediate this weakness. As of September 2021, the CIOO had completed assessments for 8 of its 14 cloud based systems, and had either initiated or planned assessments for the remaining 6 systems. The FDIC estimates it will complete corrective actions for this finding by December 2021.

In its Top Management and Performance Challenges report for 2020, the OIG considered it a weakness for the FDIC that the cloud-based systems had not been subject to annual control assessments.[67] Without annual control assessments, the FDIC has reduced assurance that it will timely identify and remediate security and privacy weaknesses that can threaten the confidentiality, integrity, and availability of cloud-based systems.

Inadequate Oversight and Monitoring of Information Systems

FISMA requires Federal agencies to implement an information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by contractors and other entities. According to NIST, outsourced information systems and services can pose unique security risks because they are not always developed or operated by agency personnel or at agency facilities, and may not benefit from the common security controls that typically protect the agency's information systems and data. FISMA and OMB policy require agencies to ensure that vendors handling sensitive information and operating systems on behalf of the Federal government meet the same security and privacy requirements as Federal agencies.

In our FISMA audit report issued in 2015,[68] we reported that the FDIC had not performed security assessments of its outsourced information systems in a timely manner as required by the FDIC's *Outsourced Information Service Provider Assessment Methodology* (OISPAM). We made a

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

[68] FDIC OIG Report, *Audit of the FDIC's Information Security Program—2015* (Report No. AUD-16-001, October 2015).

recommendation in our FISMA audit report issued in 2015 that the CIO assess its *Outsourced Information Service Provider Assessment Methodology* to determine and implement any needed improvements to ensure the timely completion of these assessments.[69] In response to our recommendation, the CIOO took several actions, including the replacement of the OISPAM with a new *Outsourced Solution Assessment Methodology* (OSAM) in November 2018.

However, during our field work of FY 2020 FISMA audit, the CIOO rescinded OSAM. According to the CISO, the approach defined in OSAM for conducting security assessments of outsourced providers did not align with the RMF [70] defined in NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations* (December 2018). Notably, the CISO determined that some of the outsourced services covered by the legacy OSAM had not been properly categorized as contractor systems. As a result, the FDIC had not conducted proper security risk assessments over these systems, nor authorization to operate, or ongoing monitoring as required by the RMF. OMB Circular A-130 requires Federal agencies to follow the RMF. The OIG identified the oversight and monitoring of outsourced systems as a weakness for the FDIC in its Top Management and Performance Challenges for 2020.[71]

As of FY 2021, the OCISO is still in the process of implementing RMF for all of its systems. This includes conducting a full review of the FDIC's current systems inventory and outsourced services covered by legacy authorization methods to ensure that all systems are properly categorized and subject to the RMF. Additionally, the OCISO will need to assess and modify, as appropriate, existing contracts to require the use of RMF for systems. During our FY 2021 FISMA audit, as described above, we noted that nine contractor and one in-house systems within CSAM were operating in the production environment without ATOs:

- Contractor Systems

(b) (7)(E)

[redacted]

[69] This recommendation is listed in Appendix I as Recommendation 4 from the FISMA audit report issued in 2015.
[70] According to NIST SP 800-37, Rev. 2, the RMF consists of (1) preparing to execute the RMF by establishing context and priorities for managing security and privacy risks, (2) categorizing systems and data based on risk, (3) selecting and tailoring controls, (4) implementing controls, (5) assessing control effectiveness, (6) authorizing systems to operate, and (7) monitoring systems and controls on an ongoing basis.
[71] FDIC OIG Report, *Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation,* February 2021, https://www.fdicoig.gov/sites/default/files/attachments/TMPC-Final-18Feb21.pdf

(b) (7)(E)

[redacted] [redacted]

8. Anchor.fm Podcast Hosting Provider.[72]

(b) (7)(E)

[redacted] [redacted]

- In-House Developed Systems

10. Complete Discovery Source INC.[73]

Additionally, in August 2021, the FDIC OIG issued a memorandum titled *Concerns Related to the FDIC's Pending Authorization to Operate Its External Wireless Network Solution Cloud Service*.[74] As noted in the memorandum, the FDIC had deployed a cloud-based solution that allowed users to set up, monitor, and configure wireless networks in April 2019. However, the solution had not undergone an ATO as of August 2021.

If the FDIC does not consistently subject its systems that host key FDIC information and data to the RMF, it cannot ensure that security and privacy risks associated with these systems will be identified and addressed in a timely manner. The lack of adequate security oversight and monitoring of outsourced systems places the confidentiality, integrity, and availability of these systems and the data they process at risk. Further, the FDIC may not have the necessary information to make efficient and effective risk management decisions about these systems supporting their mission and business functions.

Recommendation

We recommend that the CIO:

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.

RESPOND

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

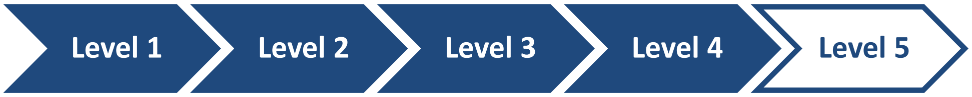
Incident Response

FISMA requires each agency to develop, document, and implement an agency-wide information security program that includes policies and procedures for incident response. In addition, NIST SP 800-61, *Computer Security Incident Handling Guide,* Rev. 2, defines procedures for establishing and training

[72] The system was decommissioned during our fieldwork period. A system description was unavailable.
[73] The system was decommissioned during our fieldwork period. A system description was unavailable.
[74] FDIC OIG Memorandum, *Concerns Related to the FDIC's Pending Authorization to Operate Its External Wireless Network Solution Cloud Service*, August 2021, https://www.fdicoig.gov/sites/default/files/publications/AEC-Memorandum-21-001_0.pdf

incident response teams; 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.

Figure 10: Maturity Rating – Incident Response



The FDIC is operating at a Maturity Level 4 (*Managed and Measurable*) in the *Incident Response* domain.

The FDIC established policies and procedures for responding to computer security incidents;[75] issued an updated agency-wide Incident Response Plan and Breach Response Plan; operated a centralized system to track and manage incidents; and implemented a CSIRT. These controls were consistent with incident response practices described in NIST SP 800-61, Rev. 2.

The FDIC utilized (b) (7)(E) [redacted] tools to enhance incident response capabilities at the FDIC. (b) (7)(E) [redacted] to provide the FDIC a holistic view of potential security incidents. The FDIC implemented its incident response plan, policy, and procedures to classify and report incidents consistent with the Attack Vectors Taxonomy and reporting timeframe defined by the United States Computer Emergency Readiness Team (US-CERT).

Recover

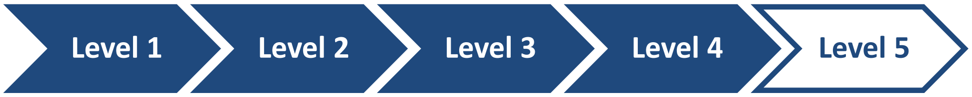
The objective of the *Recover* function is to develop and implement activities to maintain plans for resilience and to restore capabilities or services impaired due to a cybersecurity incident. The *Recover* function supports the timely recovery of normal operations to reduce the impact of a cybersecurity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

Contingency Planning

FISMA requires agencies to develop, document, and implement plans and procedures to ensure the continuity of operations for information systems that support the operations and assets of the organization. Contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption. NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems* (May 2010), provides guidance on contingency planning activities for information systems.

[75] FDIC Directive 1360.12, *Reporting Information Security Incidents* (April 2017), and *Security Operations Center (SOC)/ Computer Security Incident Response Team (CSIRT) Services Standard Operating Procedures (SOP)* (October 2019).

Figure 11: Maturity Rating – Contingency Planning



The FDIC is operating at a Maturity Level 4 (*Managed and Measurable*) in the *Contingency Planning* domain.

The FDIC established various contingency planning policies, procedures, and plans to support the recovery of its IT systems and applications that support mission-essential business functions.[76] This included an update to Directive 1360.13, *Continuity Implementation Program,* to reflect current processes and comply with updated NIST SPs, OMB Circulars, and Federal Continuity Directives. In addition, the FDIC performed a contingency plan test in October 2020 by failing over and failing back mission-critical and mission-essential applications from the Backup Data Center. The test included additional scenarios involving operational challenges to simulate a contingency scenario, improving upon the testing performed in the previous year. The test was performed in an entirely remote environment resulting from the pandemic-related maximum telework requirements, a scenario that did not apply in prior years' tests. The FDIC conducted a comprehensive After Action Report that described the overall success of the Disaster Recovery Team in achieving its objectives as well as the lessons learned. The After Actions Report was provided to senior management.

CONCLUSION

The FDIC established a significant number of information security program controls and practices consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines. Our report contains six new recommendations that, together with our open prior-year recommendations noted in Appendix I, other open OIG recommendations, and the FDIC's POA&Ms and information security initiatives, aim to strengthen the effectiveness of the FDIC's information security program controls and practices. The six recommendations are as follows:

1. Develop and implement SCRM processes and procedures in accordance with the Supply Chain Risk Management Program Directive and applicable government guidance.
2. Begin tracking completion of ICAM milestones of its revised ICAM Roadmap.
3. Complete implementation of the PCM process to include updating PIAs for all required systems.
4. Implement Document Labeling Guide requirements across the entire organization as dictated by business needs.
5. Perform an analysis of the feasibility of applying the Document Labeling Guide for documents that were created before the issuance of the directive.
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.

[76] Such policies and procedures included FDIC Directives 1360.13, *Information Technology Continuity Implementation Program* (June 2021); FDIC Directive 1500.6, *Continuity of Operations (COOP) Program* (November 2019); and CIOO *Policy on Disaster Recovery Waivers* (Policy No. 18-001, April 2018). Plans included IT disaster recovery plans for general support systems, such as (b) (7)(E), and contingency plans for IT systems and applications that support mission-essential functions, such as (b) (7)(E) .

APPENDIX I – STATUS OF PRIOR-YEAR FISMA RECOMMENDATIONS

The following table summarizes our determinations regarding the status of previously unaddressed recommendations from FISMA audit reports issued in 2016, 2019, and 2020.

Recommendation	Status
Report Issued in 2016, Recommendation 5 Review existing resource commitments and priorities for addressing the Data Communications (DCOM) Plan of Action and Milestones (POA&Ms) and take appropriate steps to ensure they are addressed in a timely manner.	Open
Report Issued in 2019, Recommendation 2 Monitor employee and contractor compliance with policy requirements for properly safeguarding sensitive electronic and hardcopy information.	Open
Report Issued in 2020, Recommendation 1 Ensure that risk acceptance decisions are reassessed in accordance with FDIC guidance to determine whether they remain valid and are at an acceptable level.	Closed
Report Issued in 2020, Recommendation 2 Implement control improvements to prevent the unauthorized installation of software on the FDIC network.	Closed
Report Issued in 2020, Recommendation 3 Remediate incomplete and out-of-date baseline configurations.	Open
Report Issued in 2020, Recommendation 4 Assess the effectiveness of the FDIC's controls for managing Administrative Accounts and implement control improvements.	Open
Report Issued in 2020, Recommendation 5 Implement a process to ensure that all outsourced information systems are subject to the NIST Risk Management Framework as prescribed by OMB policy.	Open
Report Issued in 2020, Recommendation 6 Ensure that the FDIC's cloud-based information systems are subject to annual security and privacy control assessments.	Open
Report Issued in 2020, Recommendation 7 Update FDIC's directive(s) related to contingency planning to reflect current business processes, requirements, and government-wide security policy and guidance.	Closed
Report Issued in 2020, Recommendation 8 Incorporate additional scenarios involving operational challenges into the FDIC's IT contingency plan testing exercises.	Closed

APPENDIX II – LIST OF ACRONYMS

Acronym	Description
APM	Acquisition Policy Manual
APT	Advanced Persistent Threat
ATO	Authorization to Operate
BAS	Benefit Allocation Systems
BOD	Binding Operational Directive
CDM	Continuous Diagnostics and Mitigation
CDO	Chief Data Officer
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CIOO	Chief Information Officer Organization
CISA	Cybersecurity and Infrastructure Agency
CISO	Chief Information Security Officer
COOP	Continuity of Operations
COTS	Commercial off the Shelf
CPO	Chief Privacy Officer
CSAM	Cyber Security Assessment and Management
CSIRT	Computer Security Incident Response Team
DCIO	Deputy Chief Information Officer
DCOM	Data Communications
(b) (7)(E)	[redacted]
DHS	Department of Homeland Security
DIT	Division of Information Technology
DLP	Data Loss Prevention
DPP	Data Protection Program
ERM	Enterprise Risk Management
FICAM	Federal Identity, Credential, and Access Management
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAO	Government Accountability Office
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive 12
ICAM	Identity, Credential, and Access Management
IG	Inspector General
IOSB	Information Operations Services Branch

ISCM	Information Security Continuous Monitoring
ISM	Information Security Manager
ISPA	Information Security and Privacy Awareness
IT	Information Technology
ITRAC	IT Risk Advisory Committee
KRI	Key Risk Indicator
LLC/JV	Limited Liability Company/Joint Venture
MEF	Mission Essential Function
(b) (7)(E)	[redacted]
MIS	Mission Integration Section
NIST	National Institute of Standards and Technology
OCISO	Office of the Chief Information Security Officer
OIG	Office of Inspector General
OISPAM	Outsourced Information Service Provider Assessment Methodology
OMB	Office of Management and Budget
OSAM	Outsourced Solution Assessment Methodology
PCM	Privacy Continuous Monitoring
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
RIMU	Records and Information Management Unit
(b) (7)(E)	[redacted]
RMF	Risk Management Framework
SAFe	Scaled Agile Framework
SAOP	Senior Agency Official for Privacy
SCRM	Supply Chain Risk Management
SIEM	Security Incident and Event Management
SOP	Standard Operating Procedure
SP	Special Publication
TIC	Trusted Internet Connection
US-CERT	United States Computer Emergency Readiness Team
VDP	Vulnerability Disclosure Policy

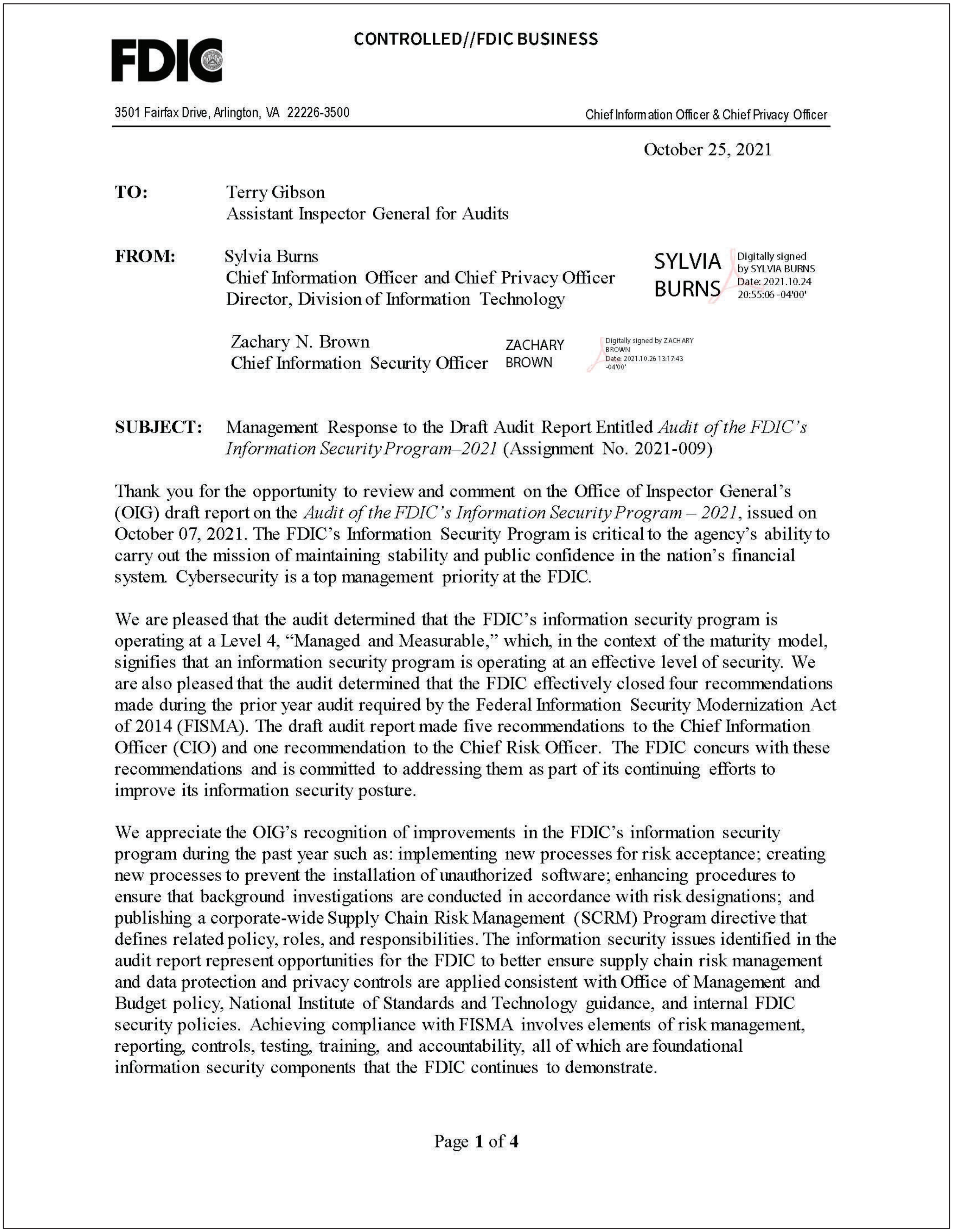
Part II

☆☆☆☆☆☆☆☆

FDIC Comments and OIG Evaluation

FDIC Comments and OIG Evaluation

The FDIC's Chief Information Officer (CIO) and Chief Information Security Officer (CISO) provided a written response, dated October 25, 2021, to a draft of the report. The response is presented in its entirety beginning on page II-2. In the response, the CIO and CISO concurred with all six of 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 begins on page II-6.



CONTROLLED//FDIC BUSINESS

FDIC

3501 Fairfax Drive, Arlington, VA 22226-3500

Chief Information Officer & Chief Privacy Officer

October 25, 2021

TO: Terry Gibson
Assistant Inspector General for Audits

FROM: Sylvia Burns
Chief Information Officer and Chief Privacy Officer
Director, Division of Information Technology

SYLVIA BURNS Digitally signed by SYLVIA BURNS Date: 2021.10.24 20:55:06 -04'00'

Zachary N. Brown
Chief Information Security Officer

ZACHARY BROWN Digitally signed by ZACHARY BROWN Date: 2021.10.26 13:17:43 -04'00'

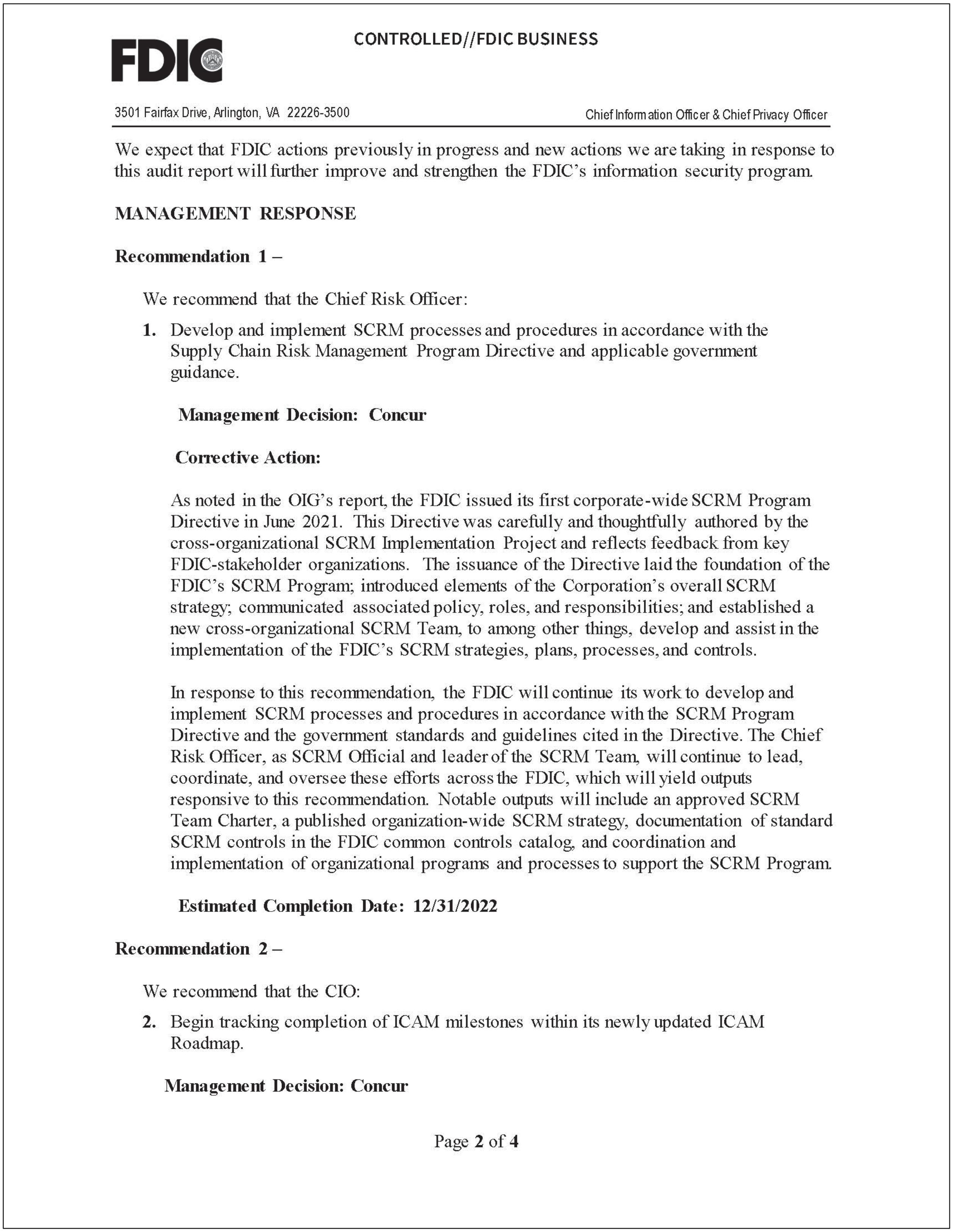
SUBJECT: Management Response to the Draft Audit Report Entitled *Audit of the FDIC's Information Security Program–2021* (Assignment No. 2021-009)

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) draft report on the *Audit of the FDIC's Information Security Program – 2021*, issued on October 07, 2021. The FDIC's Information Security Program is critical to the agency's ability to carry out the mission of maintaining stability and public confidence in the nation's financial system. Cybersecurity is a top management priority at the FDIC.

We are pleased that the audit determined that the FDIC's information security program is operating at a Level 4, "Managed and Measurable," which, in the context of the maturity model, signifies that an information security program is operating at an effective level of security. We are also pleased that the audit determined that the FDIC effectively closed four recommendations made during the prior year audit required by the Federal Information Security Modernization Act of 2014 (FISMA). The draft audit report made five recommendations to the Chief Information Officer (CIO) and one recommendation to the Chief Risk Officer. The FDIC concurs with these recommendations and is committed to addressing them as part of its continuing efforts to improve its information security posture.

We appreciate the OIG's recognition of improvements in the FDIC's information security program during the past year such as: implementing new processes for risk acceptance; creating new processes to prevent the installation of unauthorized software; enhancing procedures to ensure that background investigations are conducted in accordance with risk designations; and publishing a corporate-wide Supply Chain Risk Management (SCRM) Program directive that defines related policy, roles, and responsibilities. The information security issues identified in the audit report represent opportunities for the FDIC to better ensure supply chain risk management and data protection and privacy controls are applied consistent with Office of Management and Budget policy, National Institute of Standards and Technology guidance, and internal FDIC security policies. Achieving compliance with FISMA involves elements of risk management, reporting, controls, testing, training, and accountability, all of which are foundational information security components that the FDIC continues to demonstrate.

Page **1** of **4**



We expect that FDIC actions previously in progress and new actions we are taking in response to this audit report will further improve and strengthen the FDIC's information security program.

MANAGEMENT RESPONSE

Recommendation 1 –

We recommend that the Chief Risk Officer:

1. Develop and implement SCRM processes and procedures in accordance with the Supply Chain Risk Management Program Directive and applicable government guidance.

Management Decision: Concur

Corrective Action:

As noted in the OIG's report, the FDIC issued its first corporate-wide SCRM Program Directive in June 2021. This Directive was carefully and thoughtfully authored by the cross-organizational SCRM Implementation Project and reflects feedback from key FDIC-stakeholder organizations. The issuance of the Directive laid the foundation of the FDIC's SCRM Program; introduced elements of the Corporation's overall SCRM strategy; communicated associated policy, roles, and responsibilities; and established a new cross-organizational SCRM Team, to among other things, develop and assist in the implementation of the FDIC's SCRM strategies, plans, processes, and controls.

In response to this recommendation, the FDIC will continue its work to develop and implement SCRM processes and procedures in accordance with the SCRM Program Directive and the government standards and guidelines cited in the Directive. The Chief Risk Officer, as SCRM Official and leader of the SCRM Team, will continue to lead, coordinate, and oversee these efforts across the FDIC, which will yield outputs responsive to this recommendation. Notable outputs will include an approved SCRM Team Charter, a published organization-wide SCRM strategy, documentation of standard SCRM controls in the FDIC common controls catalog, and coordination and implementation of organizational programs and processes to support the SCRM Program.

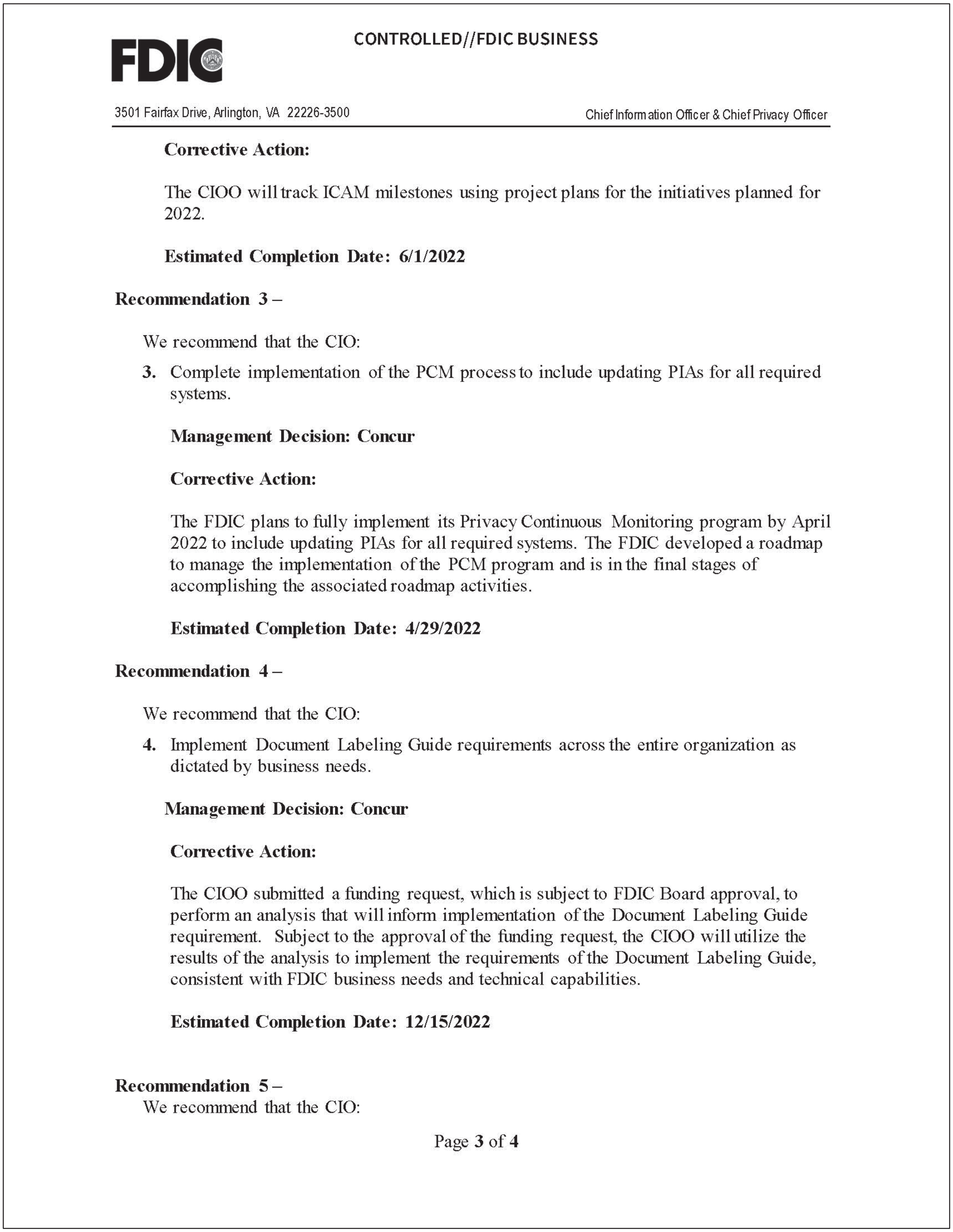
Estimated Completion Date: 12/31/2022

Recommendation 2 –

We recommend that the CIO:

2. Begin tracking completion of ICAM milestones within its newly updated ICAM Roadmap.

Management Decision: Concur



Corrective Action:

The CIOO will track ICAM milestones using project plans for the initiatives planned for 2022.

Estimated Completion Date: 6/1/2022

Recommendation 3 –

We recommend that the CIO:

3. Complete implementation of the PCM process to include updating PIAs for all required systems.

Management Decision: Concur

Corrective Action:

The FDIC plans to fully implement its Privacy Continuous Monitoring program by April 2022 to include updating PIAs for all required systems. The FDIC developed a roadmap to manage the implementation of the PCM program and is in the final stages of accomplishing the associated roadmap activities.

Estimated Completion Date: 4/29/2022

Recommendation 4 –

We recommend that the CIO:

4. Implement Document Labeling Guide requirements across the entire organization as dictated by business needs.

Management Decision: Concur

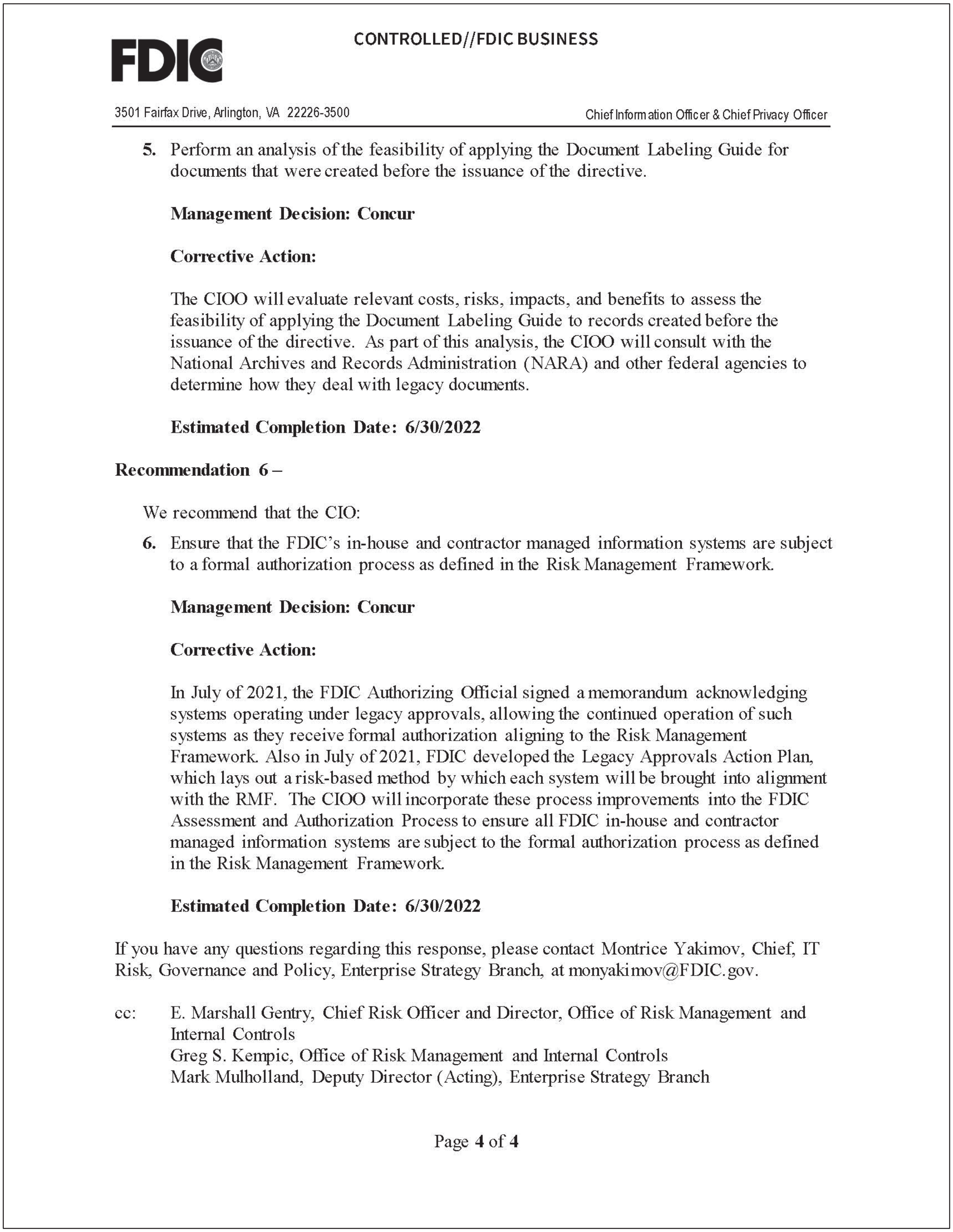
Corrective Action:

The CIOO submitted a funding request, which is subject to FDIC Board approval, to perform an analysis that will inform implementation of the Document Labeling Guide requirement. Subject to the approval of the funding request, the CIOO will utilize the results of the analysis to implement the requirements of the Document Labeling Guide, consistent with FDIC business needs and technical capabilities.

Estimated Completion Date: 12/15/2022

Recommendation 5 –

We recommend that the CIO:



CONTROLLED//FDIC BUSINESS

3501 Fairfax Drive, Arlington, VA 22226-3500

Chief Information Officer & Chief Privacy Officer

5. Perform an analysis of the feasibility of applying the Document Labeling Guide for documents that were created before the issuance of the directive.

   Management Decision: Concur

   Corrective Action:

   The CIOO will evaluate relevant costs, risks, impacts, and benefits to assess the feasibility of applying the Document Labeling Guide to records created before the issuance of the directive. As part of this analysis, the CIOO will consult with the National Archives and Records Administration (NARA) and other federal agencies to determine how they deal with legacy documents.

   Estimated Completion Date: 6/30/2022

Recommendation 6 –

We recommend that the CIO:

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.

   Management Decision: Concur

   Corrective Action:

   In July of 2021, the FDIC Authorizing Official signed a memorandum acknowledging systems operating under legacy approvals, allowing the continued operation of such systems as they receive formal authorization aligning to the Risk Management Framework. Also in July of 2021, FDIC developed the Legacy Approvals Action Plan, which lays out a risk-based method by which each system will be brought into alignment with the RMF. The CIOO will incorporate these process improvements into the FDIC Assessment and Authorization Process to ensure all FDIC in-house and contractor managed information systems are subject to the formal authorization process as defined in the Risk Management Framework.

   Estimated Completion Date: 6/30/2022

If you have any questions regarding this response, please contact Montrice Yakimov, Chief, IT Risk, Governance and Policy, Enterprise Strategy Branch, at monyakimov@FDIC.gov.

cc: E. Marshall Gentry, Chief Risk Officer and Director, Office of Risk Management and Internal Controls
Greg S. Kempic, Office of Risk Management and Internal Controls
Mark Mulholland, Deputy Director (Acting), Enterprise Strategy Branch

Page **4** of **4**

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 FDIC will continue its work to develop and implement SCRM processes and procedures in accordance with the SCRM Program Directive and the government standards and guidelines cited in the Directive. The Chief Risk Officer, as SCRM Official and leader of the SCRM Team, will continue to lead, coordinate, and oversee these efforts across the FDIC, which will yield outputs responsive to this recommendation. Notable outputs will include an approved SCRM Team Charter, a published organization-wide SCRM strategy, documentation of standard SCRM controls in the FDIC common controls catalog, and coordination and implementation of organizational programs and processes to support the SCRM Program.	December 31, 2022	$0	Yes	Open
2	The CIOO will track ICAM milestones using project plans for the initiatives planned for 2022.	June 1, 2022	$0	Yes	Open
3	The FDIC plans to fully implement its Privacy Continuous Monitoring program by April 2022 to include updating PIAs for all required systems. The FDIC developed a roadmap to manage the implementation of the PCM program and is in the final stages of accomplishing the associated roadmap activities.	April 29, 2022	$0	Yes	Open
4	The CIOO submitted a funding request, which is subject to FDIC Board approval, to perform an analysis that will inform implementation of the Document Labeling Guide requirement. Subject to the approval of the funding request, the CIOO will utilize the results of the analysis to implement the requirements of the Document Labeling Guide, consistent with FDIC business needs and technical capabilities.	December 15, 2022	$0	Yes	Open

5	The CIOO will evaluate relevant costs, risks, impacts, and benefits to assess the feasibility of applying the Document Labeling Guide to records created before the issuance of the Directive. As part of this analysis, the CIOO will consult with the National Archives and Records Administration (NARA) and other federal agencies to determine how they deal with legacy documents.	June 30, 2022	$0	Yes	Open
6	In July of 2021, the FDIC developed the Legacy Approvals Action Plan, which lays out a risk-based method by which each system will be brought into alignment with the RMF. The CIOO will incorporate these process improvements into the FDIC Assessment and Authorization Process to ensure all FDIC in-house and contractor managed information systems are subject to the formal authorization process as defined in the RMF.	June 30, 2022	$0	Yes	Open

[a] Recommendations are resolved when —

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

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

Office of Inspector General

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	Twitter	OVERSIGHT.GOV ALL FEDERAL INSPECTOR GENERAL REPORTS IN ONE PLACE
www.fdicoig.gov	@FDIC_OIG	www.oversight.gov/