The FDIC's Information Security Program–2020

October 2020 **AUD-21-001**

Audit Report

Information Technology Audits and Cyber

☆☆☆☆☆☆☆☆

REDACTED VERSION

PUBLICLY AVAILABLE

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

Office of Inspector General

Executive Summary

The FDIC's Information Security Program–2020

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

The objective of the audit was to evaluate the effectiveness of the FDIC's information security program and practices. Cotton & Company LLP planned and conducted its work based on the Department of Homeland Security's (DHS) reporting metrics: *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* Version 4.0 (April 2020) (IG FISMA Reporting Metrics).

The IG FISMA Reporting Metrics require IGs to assess the effectiveness of their agencies' 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. 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. Maturity Levels 4 and 5 are considered to be effective levels of security.

Results

Applying the IG FISMA Reporting Metrics, the FDIC's overall information security program was operating at a Maturity Level 3 (Consistently Implemented). According to the metrics, information security programs operating at this level of maturity are not considered to be effective. The table below presents the maturity level ratings assigned to the five function areas and to the overall program.

Function Area	Maturity Rating
Identify	3 (Consistently Implemented)
Protect	2 (Defined)
Detect	2 (Defined)
Respond	4 (Managed and Measurable)
Recover	3 (Consistently Implemented)
Overall Rating	**3 (Consistently Implemented)**

The FDIC established a number of information security program controls and practices that were consistent with FISMA requirements, OMB policy and guidelines, and NIST security standards and guidelines. In addition, the FDIC completed actions to address 10 of 12 unimplemented recommendations made in prior-year FISMA audit reports; implemented a process to evaluate and report whether key information technology (IT) risks were within the FDIC's Risk Appetite and established Risk Tolerance levels; developed new or revised policies and procedures in key security control areas; completed work on a new backup data center; and strengthened monitoring practices to ensure that network users complete required IT security and privacy awareness training.

However, the FISMA report describes security control weaknesses that limited the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at risk. A brief description of the highest risk security control weaknesses in the report follows.

Risk Management (Identify). The Identify function consists of processes and activities for managing IT and cybersecurity risks. The IG FISMA Reporting Metrics state that agency IGs will determine maturity ratings for each function area using a simple majority of ratings for the underlying component metrics. Therefore, applying this DHS guidance resulted in a simple mathematical determination of a Maturity Level 3 for the Identify function, because the majority of component DHS metrics in this area were operating at that level. Notwithstanding this determination, we have concerns about risk management at the FDIC, particularly because we found that the FDIC had not fully defined its Enterprise Risk Management governance, roles, and responsibilities. In addition, the FDIC had not yet implemented recommendations to integrate privacy into its Risk Management Framework (RMF), nor did the FDIC always address Plans of Action and Milestones in a timely manner. Further, the FDIC did not consistently reassess its risk acceptance decisions.

Risk Acceptance Decisions Not Consistently Reassessed (Identify). NIST guidance states that organizations should monitor their risk acceptance decisions because ongoing changes to the organization's information systems and IT environment can undermine risk assumptions. FDIC guidance states that risk acceptance decisions must be captured in an Acceptance of Risk (AR) document and reviewed periodically to ensure the ARs remain valid. The FDIC did not consistently review its existing ARs after they were initially established, or submit ARs to the FDIC's Authorizing Official for re-approval. Unless the FDIC consistently

implements a process for periodically reviewing and re-approving ARs, it cannot effectively assess the level of risk it is incurring relative to established Risk Tolerance levels.

Unauthorized Software on the Network (Protect). The FDIC has established governance processes and procedures to review and authorize software before it is installed on the network. However, these procedures and processes were not always effective. In May 2020, the FDIC discovered an unauthorized commercial software application installed on 32 desktop workstations. According to a report about this incident prepared by the FDIC, the application had not been approved by the FDIC's IT governance bodies or subject to established configuration management processes designed to ensure that only authorized software is installed on the network. Notably, in June 2019, the FDIC's Office of the Chief Information Security Officer (OCSIO) had reviewed a request to acquire this same application and recommended that alternative solutions be considered due to security concerns. The FDIC removed the unauthorized software from the 32 workstations. However, the use of unauthorized software increased the risk of a security incident and an interruption to the safe operation of the FDIC's network and applications.

Privacy Control Weaknesses Not Fully Addressed (Protect). The FDIC established a number of data protection and privacy controls. However, the FDIC had not yet completed actions to address privacy control weaknesses identified in our audit report on the FDIC's Privacy Program issued in December 2019. Specifically, the FDIC had not:

- Fully integrated privacy considerations into its RMF designed to establish privacy plans and select and continuously monitor system privacy controls;
- Implemented its planned Document Labeling initiative designed to identify, categorize, label, and protect sensitive information, including personally identifiable information (PII);
- Established controls to effectively manage and secure PII stored in network shared drives; or
- Completed action to ensure that PII is disposed of within established timeframes.

As of August 31, 2020, the FDIC had not addressed 12 of the 14 recommendations contained in our Privacy Program audit report.

Oversight and Monitoring of Outsourced Systems Not Adequate (Detect). 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. In June 2020, the FDIC rescinded its *Outsourced Solution Assessment Methodology* (OSAM) used to assess security and privacy risks associated with outsourced information systems. According to the

Chief Information Security Officer (CISO), the OSAM did not align with the NIST RMF guidance. As a result, the FDIC had not properly categorized some of its systems covered by OSAM or subject these systems to a proper risk assessment, authorization to operate, or ongoing monitoring. Until the FDIC subjects all of its outsourced systems to the RMF, the FDIC cannot be sure that it will identify and address security and privacy risks in a timely manner.

Cloud-based Systems Not Subject to Annual Control Assessments (Detect). FISMA requires Federal agencies to test and evaluate the effectiveness of their information system security controls on a frequency no less than annually. FDIC guidance requires security and privacy controls for cloud-based systems to be assessed on a 3-year cycle, with at least some controls tested each year. As of April 1, 2020, the FDIC had 14 cloud-based systems that provided critical IT services, such as [redacted]. The FDIC did not subject these cloud-based systems to annual control assessments. In two cases, the FDIC had not completed annual control assessments for more than 3 years after the FDIC authorized the systems to operate. 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.

Recommendations

The FISMA report contains eight recommendations addressed to the FDIC's Chief Information Officer. The report recommends that the FDIC reassess its risk acceptance decisions in accordance with guidance; implement control improvements to prevent the unauthorized installation of software on the network; and complete actions to address open Plans of Action and Milestones related to baseline configurations. The report also recommends that the FDIC assess and improve controls for managing administrative accounts; implement a process to ensure all outsourced information systems are subject to the RMF; and ensure all cloud-based systems are subject to annual security and privacy control assessments. Finally, the report recommends that the FDIC update its IT contingency planning policy and incorporate additional scenarios into its IT contingency plan testing. The FDIC concurred with all eight of the report's recommendations and plans to complete corrective actions by December 31, 2021.

Contents

Part I

☆☆☆☆☆☆☆☆

Report by Cotton & Company LLP

THE FEDERAL DEPOSIT INSURANCE CORPORATION'S INFORMATION SECURITY PROGRAM – 2020

AUDIT REPORT

OCTOBER 27, 2020

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

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

Mark F. Mulholland
Assistant Inspector General for IT Audits and Cyber
Office of Inspector General
Federal Deposit Insurance Corporation

Subject: Audit of the Federal Deposit Insurance Corporation's Information Security Program – 2020

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-0479-0002. Cotton & Company LLP performed the work from April through September 2020.

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,

Loren Schwartz, CPA, CISSP, CISA
Partner

INTRODUCTION

According to the Office of Management and Budget (OMB), America's infrastructure, both public and private, continues to be a top target of malicious cyber actors, intent on disrupting the geopolitical and socioeconomic stability and prosperity of the United States.[1] Every day, Federal agencies defend their information systems and data against cyberattacks. OMB reported that Federal agencies experienced 28,581 cybersecurity incidents during Fiscal Year (FY) 2019.[2]

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. Absent effective controls for safeguarding its information systems and data, the FDIC is 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)[3] requires Federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. FISMA directs 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 documents 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 2019.
[2] OMB, *Federal Information Security Modernization Act of 2014 Annual Report to Congress*, Fiscal Year 2019.
[3] Pub. L. No. 113-283 (December 2014). FISMA's obligations for Federal agencies and for Federal Inspectors General, as relevant to this audit, are codified chiefly to 44 U.S.C. §§ 3554 and 3555, respectively. The FDIC has determined that FISMA is legally binding on the FDIC.

- 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),[4] requires Federal agencies to use the NIST Cybersecurity Framework to manage their cybersecurity risks. As described later, 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 all 5 components of internal control, and all 17 associated principles, defined in the Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* (September 2014) (Green Book).[5] Our assessment of internal controls was based on the DHS *Fiscal Year (FY) 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting*

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

[5] The Green Book organizes internal control through a hierarchical structure of five components and 17 principles. The five components, which represent the highest level of the hierarchy, 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.

Metrics Version 4.0 (April 2020) (IG FISMA Reporting Metrics). Accordingly, our work may not have identified all internal control deficiencies in the FDIC's information security program and practices that existed at the time of our audit.

To accomplish our objective, we:

- Evaluated key components of the FDIC's information security program plans, policies, procedures, and practices that were in place as of July 8, 2020 (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-20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements* (November 2019), when planning and conducting our work.
- Assessed the maturity of the FDIC's information security program with respect to the metrics defined in the IG FISMA Reporting Metrics. As discussed later, the IG FISMA Reporting Metrics provide a framework for assessing the effectiveness of agency information security programs.
- Selected and evaluated security controls related to a non-statistical sample of three FDIC-maintained information systems and one contractor system (listed below). Our analysis of these systems included reviewing selected system documentation and other relevant information, as well as testing selected security controls.

  FDIC-Maintained Information Systems

  - *Data Communications (DCOM)*
    DCOM consists of critical network infrastructure components, such as firewalls, routers, and switches, that support the safe and continued operation of the FDIC's network information technology (IT) environment. DCOM also consists of the interfaces between the FDIC's network and the Internet, external systems and networks, and remote users.
  - *Windows Servers*
    Servers running the Microsoft Windows Server operating system (Windows Servers) support mission-essential FDIC systems, business applications, and services. Windows Servers also store and process large quantities of sensitive FDIC information, including PII, confidential bank examination information, lists of banks scheduled for closing, and plans for the resolution of systemically important financial institutions.
  - *Claims Administration System (CAS)*
    CAS is a mission-essential system that FDIC personnel use to support the resolution of insured financial institutions. The FDIC uses CAS for such things as estimating the amount of uninsured deposits in order to determine the least costly form of resolution, and processing and tracking deposit insurance claims. CAS provides a repository of sensitive depositor information related to failed financial institutions.

  Contractor System

  - *Advanced Legal Information System (ALIS)*
    ALIS is an externally hosted, web-based application designed to assist managers, supervisors, attorneys and support staff in the Legal Division with the management of legal matters. ALIS supports the creation, management, and tracking of legal matters and legal activities. ALIS also has the ability to create, manage, and exchange data on

invoices and payments to outside counsel and legal services support providers, as well as timekeeping and tracking of the activities and functions in support of the Legal Division's needs.

We selected the systems described above because they contain large quantities of sensitive information and support mission-essential functions. A disruption of these systems could impair the FDIC's ability to achieve its mission.

As part of the audit, we 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. Cotton & Company LLP conducted the audit remotely at its off-site locations in the Washington, D.C. metropolitan area from April through September 2020.

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

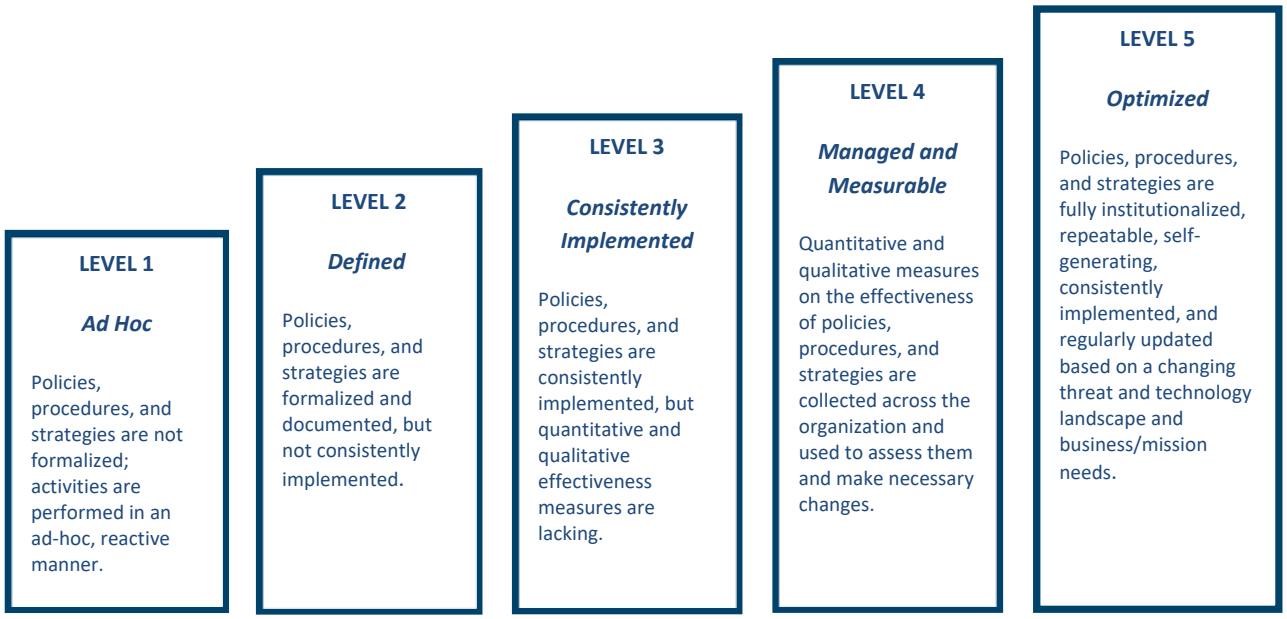
Table 1: Alignment of the NIST Cybersecurity Framework Function Areas with the IG FISMA Reporting Metric Domains

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**
Protect	Implement safeguards to ensure delivery of critical infrastructure services, as well as to prevent, limit, or contain the impact of a cybersecurity event.	**Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training**
Detect	Implement activities to identify the occurrence of cybersecurity events.	**Information Security Continuous Monitoring (ISCM)**
Respond	Implement processes to take action regarding a detected cybersecurity event.	**Incident Response**
Recover	Implement plans for resilience to restore any capabilities impaired by a cybersecurity event.	**Contingency Planning**

Source: Cotton & Company LLP analysis of the NIST Cybersecurity Framework and IG FISMA Reporting Metrics.

The IG FISMA Reporting Metrics require IGs to assess the effectiveness of their agency's information security programs 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 IG 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



Source: IG FISMA Reporting Metrics.

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.

[6] More information regarding how Inspectors General are to determine maturity level ratings can be found at https://www.cisa.gov/publication/fy20-fisma-documents.

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

The FDIC's Chief Information Security Officer (CISO), who reports directly to the CIO, is delegated responsibility for planning, developing, and implementing an agency-wide information security program. 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. The FDIC has Information Security Managers (ISM) within the Division of Insurance and Research, Division of Administration, Division of Finance, Division of Resolutions and Receiverships, Division of Depositor and Consumer Protection, Division of Risk Management Supervision, Legal Division, Division of Complex Institution Supervision & Resolution, DIT, OCISO, and OIG. ISMs provide a security focus within their respective Divisions and Offices and educate employees and contractors who have access to systems and data. ISMs assess the level of security in applications and service providers; ensure their Division or Office addresses security requirements in new or enhanced systems; and promote compliance with FDIC security policies and procedures, among other security tasks.

CIOO Reorganization

In November 2019, FDIC management approved a plan to reorganize the CIOO. According to the FDIC, the reorganization was intended to: (a) improve IT services and the customer experience; (b) streamline IT management and operations; (c) provide a single path for the intake, prioritization, and assignment of new IT work from business stakeholders; and (d) strengthen the CIOO workforce planning functions. In May 2020, FDIC management approved an updated reorganization, which outlines the future state of the CIOO. Notable organizational changes include the establishment of the following new senior leadership roles:

- Principal Deputy CIO who will report to the CIO and provide strategic leadership, oversight, and management direction/guidance to members of the CIOO's Senior Leadership Team. Although the FDIC has hired a Principal Deputy CIO as of July 5, 2020, the individual selected for the position is currently on detail to another Federal agency until November 2020.
- Chief Data Officer (CDO) and supporting staff who will work to align the data-related functions across the organization and address a vision for data management.

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

The CIOO completed its reorganization, including administrative processes and reassigning staff, on September 27, 2020.

SUMMARY OF RESULTS

Based on the results of our audit work and the application of the IG FISMA Reporting Metrics, we determined that the FDIC's information security program is operating at a Maturity Level 3 (*Consistently Implemented*). According to the IG FISMA Reporting Metrics, organizations operating at a Maturity Level 3 are not considered to have an effective information security program. 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.

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	3
Protect	Configuration Management	2	2	
	Identity and Access Management	2		
	Data Protection and Privacy	2		
	Security Training	4		
Detect	ISCM	2	2	
Respond	Incident Response	4	4	
Recover	Contingency Planning	3	3	

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

Note: Consistent with the guidance in the IG 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. We also considered the FDIC's unique mission, resources, and challenges when determining maturity ratings.

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 2019. For example, the FDIC:

- Completed actions to address 10 of 12 unimplemented recommendations made in prior-year FISMA audit reports.
- Implemented a process to evaluate and report whether key IT risks were within the FDIC's Risk Appetite and established Risk Tolerance levels.[8]

[8] OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (OMB Circular A-123, July 2016), states that Risk Appetite serves as a guidepost to establish strategy and select objectives and a Risk Tolerance. OMB Circular A-123 states that Risk Tolerance is the acceptable level of variance in performance relative to the achievement of objectives.

- Developed new or revised procedures in key security control areas, including system authorizations;[9] Plans of Action and Milestones (POA&M)[10] management; patch management; and security and privacy control assessments.
- Completed work on a new Backup Data Center intended to help ensure IT systems and applications supporting mission-essential business functions can be recovered within targeted timeframes.
- Strengthened monitoring practices to ensure that network users complete required IT security and privacy awareness training.

Notwithstanding these actions, our report describes security control weaknesses that limited the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at risk. In some cases, these security control weaknesses were identified during separate OIG audits and evaluations that were either ongoing or completed, or through security and privacy control assessments completed by the FDIC. Because the FDIC had not yet completed corrective action 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 posed the most risk of impacting the confidentiality, integrity, or availability of FDIC information systems and data follows. In addition, Appendix I contains the status of recommendations made in FISMA audit reports issued in prior years.

ERM Governance, Roles, and Responsibilities Not Fully Defined (Identify – Risk Management). OMB Circular A-123 requires Federal agencies to implement an Enterprise Risk Management (ERM) capability. OMB Circular A-123 also encourages Federal agencies to establish a risk management governance structure that includes a Risk Management Council. In July 2020, the FDIC OIG issued an evaluation report on the FDIC's implementation of ERM (ERM Report). The ERM Report stated that the FDIC had not established clear oversight authorities, roles, and responsibilities for the FDIC Operating Committee, which serves as the Risk Management Council for the FDIC. The FDIC had also not defined clear roles, responsibilities, and processes for its Board of Directors and various committees and groups involved in ERM. The ERM Report concluded that well-defined authorities, roles, and responsibilities would help ensure the range of risks facing the FDIC are properly identified and managed. The ERM Report contained a total of eight recommendations. The FDIC concurred with five of the eight recommendations, and non-concurred with the remaining three recommendations.

Risk Acceptance Decisions Not Consistently Reassessed (Identify – Risk Management). NIST guidance states that organizations should monitor their risk acceptance decisions because ongoing changes to the organization's information systems and IT environment can undermine risk assumptions. FDIC guidance

[9] OMB Circular A-130 requires Federal agencies to authorize their information systems to operate. A senior management official (the Authorizing Official) reviews security-related information describing the security posture of systems, and using that information, determines whether the risk to mission/business operations is acceptable. If the Authorizing Official determines that the risk is acceptable, then the official explicitly accepts the risk. At the FDIC, the CIO functions as the Authorizing Official.

[10] A POA&M is a management tool used by agency CIOs, security personnel, program officials, and others to track the progress of corrective actions pertaining to security vulnerabilities identified through security control assessments and other sources. POA&Ms assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective actions pertaining to security vulnerabilities.

states that risk acceptance decisions must be captured in an Acceptance of Risk (AR)[11] document and reviewed periodically to ensure the ARs remain valid. We found that the FDIC did not consistently review its existing ARs after they were initially established, or consistently submit ARs to the Authorizing Official for re-approval. Unless the FDIC consistently implements a process for regularly reviewing and re-approving ARs, it cannot effectively assess the level of risk it is incurring relative to established Risk Tolerance levels.

Unauthorized Software on the Network (Protect – Configuration Management). The FDIC has established governance processes and procedures to review and authorize software before it is installed on the network. However, these processes and procedures were not always effective. In May 2020, the FDIC discovered an unauthorized commercial software application installed on 32 desktop workstations. According to a report about this incident prepared by the FDIC, the application had not been approved by the FDIC's IT governance bodies or subject to established configuration management processes designed to ensure that only authorized software is installed on the network. Notably, in June 2019, the OCISO had reviewed a request to acquire this same application and recommended that alternative solutions be considered due to security concerns. The FDIC removed the unauthorized application from the 32 workstations. The use of unauthorized software increases the risk of a security incident and an interruption to the safe operation of the FDIC's network and applications.

Privacy Control Weaknesses Not Fully Addressed (Protect – Data Protection and Privacy). The FDIC established a number of data protection and privacy controls, including a Privacy Program Policy, Privacy Program Plan, Breach Response Plan, and privacy training and awareness program. However, the FDIC had not yet completed actions to address a number of privacy control weaknesses identified in an FDIC OIG audit report issued in December 2019.[12] For example, the FDIC had not fully integrated privacy considerations into its Risk Management Framework (RMF);[13] implemented its planned Document Labeling initiative (formerly known as the Data Protection Program) to identify, categorize, label, and protect PII and sensitive information; established controls to effectively manage and secure PII stored in network shared drives; or completed action to ensure that PII is disposed of within established timeframes. The OIG's audit report contained 14 recommendations. As of August 31, 2020, the OIG had closed 2 of the 14 recommendations. The other 12 recommendations remain unimplemented. Weaknesses in the FDIC's Privacy Program increased the risk of PII loss, theft, and unauthorized access or disclosure.

Oversight and Monitoring of Outsourced Systems Not Adequate (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. We had previously made a recommendation in our FISMA audit report issued in 2015 that the CIO assess its

[11] An AR is a memorandum signed by the CIO, CISO, and other FDIC IT professionals that describes a known security weakness or vulnerability for which the FDIC has reviewed mitigation controls, decided not to pursue further remediation, and accepted the residual risk.
[12] FDIC OIG Report, *The FDIC's Privacy Program* (Report No. AUD-20-003, December 2019).
[13] NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations*, defines the RMF as a structured process that integrates information security, privacy, and risk management activities into the information system development lifecycle. OMB Circular No. A-130, *Managing Information as a Strategic Resource* (July 2016, OMB Circular A-130) requires Federal agencies to implement NIST's RMF. The FDIC has determined that OMB Circular A-130 is "generally applicable" to the FDIC, to the extent that the Circular aligns with OMB's statutory authorities, does not impose obligations on the FDIC based on statutes that are legally inapplicable to the FDIC, and does not conflict with the FDIC's independence, statutory obligations, or regulatory authority. FDIC Review of OMB Circular A-130 (July 28, 2016).

Outsourced Information Service Provider Assessment Methodology (OISPAM) to determine and implement any needed improvements to ensure the timely completion of the assessments. In response to this recommendation, in November 2018, the CIOO replaced the OISPAM with the *Outsourced Solution Assessment Methodology* (OSAM) to govern its assessment of security and privacy risks for outsourced information systems. The CIOO then executed a strategy to guide the transfer of outsourced service providers from the legacy OISPAM to the OSAM. The FDIC OIG closed the recommendation in April 2020.

However, in June 2020, the CISO rescinded the OSAM, because it did not align with the RMF defined in NIST guidance. As a result, the FDIC did not properly categorize some systems covered by OSAM as contractor systems, or subject these systems to a proper risk assessment, authorization to operate, or ongoing monitoring.

During our FISMA audit, OCISO staff began working with contracting officials to ensure that any new or planned contracts for outsourced systems are subject to the RMF. OCISO staff informed us that they intended to conduct a review of the FDIC's systems inventory and outsourced services covered by the legacy OSAM to ensure that all FDIC systems are properly categorized and subject to the RMF. OCISO staff also stated that they intended to integrate the RMF into the FDIC's procurement policies, processes, and guidance, and modify existing contracts to require adherence to the RMF. The OCISO has not yet determined when it plans to complete these reviews and has not yet developed milestones for these actions. Until the FDIC subjects all of its outsourced systems to the RMF, the FDIC cannot be sure it will identify and address security and privacy risks in a timely manner.

Cloud-based Systems Not Subject to Annual Control Assessments (Detect – ISCM). FISMA requires Federal agencies to test and evaluate the effectiveness of their information system security controls on a frequency no less than annually. The *FDIC Security and Privacy Control Assessment (SCA) Methodology* requires security and privacy controls for the FDIC's cloud-based information systems be assessed on a 3-year cycle, with at least some controls tested every year. 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 [redacted]. The CIOO did not subject these 14 systems to annual security and privacy control assessments. 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 September 2019, the FDIC created a POA&M to remediate this weakness. As of September 11, 2020, the CIOO had completed assessments for 4 of its 14 cloud-based systems, and had either initiated or planned assessments for the remaining 10 systems. 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.

AUDIT RESULTS

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. The NIST Cybersecurity Framework uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity.

Risk Management

The *Risk Management* domain defined in the IG 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 enterprise, business process, and system levels; implementing an information security architecture; utilizing POA&Ms to mitigate security weaknesses; performing system level risk assessments and conducting system scanning; and ensuring contracts and service-level agreements address security and privacy.

Figure 2: Maturity Rating - Risk Management

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

The IG FISMA Reporting Metrics state that agency IGs will determine maturity ratings for each domain using the simple majority of ratings for component metrics.[14] Therefore, applying this DHS guidance resulted in a simple mathematical determination of a Maturity Level 3, because the majority of DHS metrics in the *Risk Management* domain were operating at that level. We found that the FDIC had completed a Risk Inventory and Risk Profile[15] and used an automated solution to provide a centralized view of enterprise risks including remediation activities and risk scores. In addition, the FDIC established an information security risk management policy and supporting process and guidance documents;[16] and implemented processes for maintaining a comprehensive and accurate inventory of information systems, hardware, software, and software licenses. The FDIC had also performed risk assessments and scans of its systems; categorized[17] and communicated the importance and priority of its systems.

[14] The IG FISMA Reporting Metrics state agency IGs will determine maturity ratings for each domain using a simple majority, where the most frequent maturity ratings (the mode) across the domain questions will serve as the domain rating.
[15] The FDIC defines a *Risk Profile* as a prioritized list of the most significant risks identified and assessed through the risk assessment process.
[16] 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).
[17] 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.

Further, the FDIC's IT Risk Advisory Council (ITRAC)[18] monitored IT and cybersecurity risks facing the FDIC to determine whether they were within established Risk Tolerance levels and the FDIC's Risk Appetite.

However, notwithstanding this determination regarding the *Risk Management* domain, we have concerns about risk management at the FDIC, particularly because the FDIC OIG found that the FDIC had not fully defined its ERM governance, roles, and responsibilities. In addition, the FDIC had not yet completed work to fully integrate privacy into its RMF, nor did the FDIC ensure that many moderate-risk POA&Ms were addressed in a timely manner. Further, the FDIC did not consistently re-validate its prior risk acceptance decisions, or report this information to the FDIC's Authorizing Official.

ERM Governance, Roles, and Responsibilities Not Fully Defined

OMB Circular A-123 requires Federal agencies to implement an ERM capability.[19] According to OMB Circular A-123, ERM is an effective agency-wide approach to addressing the full spectrum of an organization's external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos. OMB Circular A-123 encourages Federal agencies to establish a risk management governance structure that includes a Risk Management Council.[20] The FDIC has designated the Operating Committee to serve as the FDIC's Risk Management Council and the oversight body for ERM. The Operating Committee is comprised of FDIC Division and Office Directors and Deputies to the FDIC Chairman.

In July 2020, the FDIC OIG issued an evaluation report, entitled *The FDIC's Implementation of Enterprise Risk Management* (ERM Report).[21] In its report, the OIG noted that the FDIC issued an ERM directive and procedure,[22] and made progress toward implementing ERM in compliance with government-wide guidance and best practices. However, the ERM Report stated that the FDIC needed to establish a clear governance structure, and clearly define authorities, roles, and responsibilities for ERM. Of note, the ERM Report stated that the FDIC had not established clear oversight authorities, roles, and responsibilities for the FDIC Operating Committee pertaining to ERM. The FDIC had also not defined clear roles, responsibilities, and processes for its Board of Directors and various committees and groups involved in ERM. The ERM Report concluded that well-defined authorities, roles, and responsibilities would help ensure the range of risks facing the FDIC are properly identified and managed.

The ERM Report contained a total of eight recommendations intended to strengthen the ERM Program. The report included recommendations for the FDIC to: (1) define, document, and implement the authorities, roles, and responsibilities of the Operating Committee as the Risk Management Council; (2) define the roles and responsibilities of the Board of Directors with respect to ERM, including its role in endorsing the risk appetite statement; and (3) develop and implement ERM communication protocols

[18] The ITRAC is comprised of the CIO, CISO, Chief Risk Officer (CRO), and other FDIC stakeholders.
[19] The FDIC has determined that OMB Circular A-123 is not binding on the FDIC with respect to ERM, but that the Circular provides "good government" principles that may be useful to the FDIC's own ERM program.
[20] OMB Circular A-123 states that to provide guidance for the risk management function, agencies may use a Risk Management Council to oversee the establishment of the agency's Risk Profile, regular assessment of risk, and development of appropriate risk responses.
[21] FDIC OIG Report, *The FDIC's Implementation of Enterprise Risk Management* (Report No. EVAL-20-005, July 2020).
[22] FDIC Directive 4010.3, *Enterprise Risk Management and Internal Control Program (*October 2018), and FDIC *Enterprise Risk Management Standard Operating Procedure* (May 2020).

to the Board. These recommendations are unresolved. The OIG plans to seek resolution of the unresolved recommendations through the evaluation follow-up process.

Integration of Privacy into the Risk Management Framework Incomplete

OMB Circular A-130 requires Federal agencies to use the RMF defined in NIST SP 800-37 to not only manage security risk, but privacy risk as well. According to OMB Circular A-130, agencies use the RMF to guide and inform the categorization of information and information systems; the selection, implementation, and assessment of security and privacy controls; and the continuous monitoring of security and privacy controls in information systems.

In December 2019, the FDIC OIG issued an audit report on the FDIC's Privacy Program.[23] In the report, the OIG concluded that the FDIC had not fully integrated privacy considerations into its RMF. At the close of our FISMA audit, the FDIC was working to address 12 of the 14 recommendations in the OIG's report. Notably, 2 of these 12 recommendations involved developing and approving privacy plans for all FDIC systems containing PII consistent with OMB policy, and implementing a privacy continuous monitoring program to regularly assess the effectiveness of privacy controls.

Addressing DCOM POA&Ms Incomplete

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,[24] we reported that the FDIC did not address security weaknesses with a risk rating of Moderate[25] in POA&Ms for the DCOM 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.[26]

In response to this recommendation, in March 2019 and May 2019, the CIOO updated its POA&M policy and procedures to provide guidance on establishing remediation timeframes based on risk ratings to facilitate resource allocations. However, as of August 30, 2020, the FDIC's Cyber Security Assessment and Management (CSAM) system contained [redacted] POA&Ms related to DCOM that were open. [redacted] In 2020, the CIOO established a project team to work with subject matter experts to resolve open POA&Ms related to DCOM and expects to address our prior recommendation by June 2021.

[23] FDIC OIG Report, *The FDIC's Privacy Program* (Report No. AUD-20-003, December 2019).
[24] FDIC OIG Report, *Audit of the FDIC's Information Security Program – 2016* (Report No. AUD-17-001, November 2016).
[25] The FDIC assigns risk ratings of High, Moderate, or Low to its POA&Ms. These ratings provide a framework for communicating the severity and potential impact of the weakness in the POA&M, and for prioritizing remediation activities.
[26] This recommendation is listed in Appendix I as Recommendation 5 from the FISMA audit report issued in 2016.

Risk Acceptance Decisions Not Consistently Reassessed

According to NIST SP 800-39, *Managing Information Security Risk* (March 2011), risk acceptance may be an appropriate response to an identified risk[27] when the risk falls within the organization's Risk Tolerance. If the organization decides to accept a risk, NIST SP 800-39 states that the organization should monitor the risk acceptance because ongoing changes to the organization's information systems and IT environment can undermine risk assumptions. The FDIC's *ISM Program Technical Guide for Stakeholders* (ISM Guide) defines a process for accepting identified risks. According to the ISM Guide, decisions to accept risk must be captured in an Acceptance of Risk (AR) document. Division and Office ISMs, working in coordination with OSICO staff and system owners, prepare ARs when they determine that risk acceptance is the most appropriate course of action for an identified risk. The FDIC typically identifies risks through security control assessments of its information systems and records these risks on POA&Ms. The ISM Guide requires that ARs be associated with a POA&M, stored in CSAM, and reviewed periodically to ensure they remain valid.

We reviewed information in CSAM as of July 30, 2020, for all open POA&Ms with an AR. As reflected in Table 3, CSAM did not identify the date of the FDIC's last review for 155 (21 percent) of the 723 ARs.

Table 3: Analysis of Existing ARs as of July 30, 2020

POA&M Criticality	Open POA&Ms with an AR	AR reviewed in the past 12 months	AR not reviewed in the last 12 months
Low	491	397	94
Medium	231	170	61
High	1	1	0
Total	723	568	155

Source: Cotton & Company LLP's analysis of information in CSAM as of July 30, 2020.

After we brought this matter to the FDIC's attention, on August 25, 2020, the OCISO presented materials to the FDIC's ISMs stating that many ARs from prior years had not been reviewed since they were first reported, and High/Medium Risk ARs had not been re-approved by the Authorizing Official. Regular monitoring of risk acceptance decisions helps organizations to maintain awareness of the risks they are incurring. Unless the FDIC consistently implements a process for periodically reviewing existing ARs, it cannot be sure that the risks it has accepted remain valid. Further, consistent reporting of AR information to the FDIC's Authorizing Official would help to ensure the Authorizing Official maintains knowledge of the current security state of information systems relative to established Risk Tolerance levels.

[27] NIST SP 800-39 states that organizations can respond to risk in a variety of ways, including: accepting the risk, avoiding the risk; mitigating the risk; sharing or transferring the risk to other organization(s), or a combination of these risk responses.

Recommendation

We recommend that the CIO:

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.

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 4: Maturity Rating - Configuration Management

The FDIC is operating at a Maturity Level 2 (*Defined*) in the *Configuration Management* domain.

The FDIC had 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;[28] an Infrastructure Change Control Board to review and approve changes to the IT infrastructure; and a centralized system to track, manage, and report software

[28] 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).

configuration changes. The FDIC also completed actions to address three recommendations made in prior FISMA audit reports related to patch management and vulnerability scanning of network IT devices and systems.[29] However, as described below, the FDIC did not always follow its configuration management processes, which allowed unauthorized software to be installed on its network. In addition, the FDIC had not yet completed work to develop and/or update baseline configurations for some of its network IT devices. Further, the FDIC implemented the requirements of OMB's Trusted Internet Connections (TIC) initiative at the close of our audit field work (September 2020).

Unauthorized Software Installed on the Network

The FDIC established governance processes and procedures intended to ensure that software is properly reviewed and authorized before it is introduced into the IT environment. For example, in March 2018, the FDIC established the Security and Enterprise Architecture Technical Advisory Board (SEATAB) to evaluate requests for new technologies for consistency with the FDIC's Enterprise Architecture (EA).[30] In addition, the CIOO's *Infrastructure Services Branch Change Management Procedure*, Version 2.0.1 (December 2017), requires the FDIC's Infrastructure Change Control Board to review and approve all new software before it is installed in the FDIC's IT environment.

On May 15, 2020, an FDIC employee in the Division of Complex Institution Supervision and Resolution notified the FDIC's Computer Security Incident Response Team (CSIRT) that an unauthorized commercial software application had been installed on an FDIC virtual workstation connected to the network. In response, CSIRT opened an investigation of the incident. CSIRT found that a DIT Senior IT Specialist had installed the application on 32 virtual workstations, as well as a Gold Image[31] used to configure the virtual workstations. According to a report prepared by CSIRT on this incident, the application had not been approved by the FDIC's IT governance bodies or subject to established configuration management processes. Specifically, the CSIRT report found that:

- Neither the SEATAB nor the Infrastructure Change Control Board had approved the application for use in the FDIC's IT environment.
- The application had not been subject to any of the FDIC's formal configuration management processes.
- OCISO had conducted a security review of the application and prepared a report in June 2019.[32] The OCISO's report stated that the application presented risk because it was maintained by a company in a foreign country. OCISO's report recommended that the FDIC consider alternative solutions. OCISO's report added that "all code is required to go through software quality and vulnerability checks prior to deployment on the FDIC production network."

[29] These recommendations are listed in Appendix I as Recommendations 9 and 10 from the FISMA audit report issued in 2017, and Recommendation 4 from the FISMA audit report issued in 2018.
[30] OMB Circular A-130 requires agencies to develop an EA that describes the agency's baseline architecture, target architecture, and a transition plan to attain the target architecture.
[31] A Gold Image is a pre-configured template or standard build of a virtual machine, desktop, server, or hard disk drive. IT professionals use Gold Images to create new instances of these virtual IT resources to save time and help ensure consistency in the IT environment.
[32] *FDIC Security Recommendation Report*, Version 1.0 (June 2019), prepared by OCISO's Security Architecture Section.

The installation and use of software that has not been subject to formal configuration management presents a risk to the security and operation the FDIC's network, applications, and data. In the case of the application described above, in June 2019, the OCISO had recommended that the FDIC consider alternative solutions because the application was maintained by a company in a foreign country. Based on the results of CSIRT's investigation, DIT removed the unauthorized application from the 32 workstations and Gold Image during our audit. Nevertheless, a review of the FDIC's configuration management controls is warranted.

Recommendation

We recommend that the CIO:

2. Implement control improvements to prevent the unauthorized installation of software on the FDIC network.

Baseline Configurations for Some Systems Not Fully Developed

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 formally approved, 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. 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 baseline configurations that were either incomplete or out-of-date. The POA&Ms addressed certain key network IT devices, including [redacted]. Notably, the estimated completion dates for 5 of the 13 POA&Ms were past due, and 3 were more than 200 days past due. 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.

Recommendation

We recommend that the CIO:

3. Remediate incomplete and out-of-date baseline configurations.

Trusted Internet Connection Initiative

To improve the effectiveness of information security across the Federal government, in November 2007, OMB announced the Trusted Internet Connections (TIC) initiative.[33] Initially, the TIC initiative focused on (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 would 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, because the TIC initiative was a policy initiative and not grounded in statutory authority. As a result, the FDIC did not initially implement OMB's TIC initiative.

However, in September 2019, OMB issued Memorandum 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 Memorandum 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 Memorandum M-19-26 is binding on the FDIC, because this memorandum is grounded in the statutory authority of FISMA.

OMB Memorandum M-19-26 defines an enhanced approach for implementing TIC 3.0 that provides Federal agencies with increased flexibility to use modern security capabilities. OMB Memorandum M-19-26 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 Memorandum 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 Memorandum M-19-26 requires agencies to update their network and system boundary policies, and identify appropriate TIC Use Cases[35] by September 12, 2020.

At the close of our audit field work 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 had deployed physical sensors to implement the security capabilities outlined in its TIC Use Cases.

---

[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] 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.

Identity and Access Management

Identity and Access Management involves implementing a set of capabilities to ensure that only authorized users 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.[36] 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, the NIST SP 800 series 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 executive departments and agencies for employees and contractors.

Figure 5: Maturity Rating – Identity and Access Management

The FDIC is operating at a Maturity Level 2 (*Defined*) 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 an ICAM Strategy, Program Charter, and Segment Architecture,[37] and policies and procedures for identifying, authenticating, and managing users who access FDIC information systems and facilities.[38] However, as described below, the FDIC did not always maintain Confidentiality Agreements for its contractor personnel as required by FDIC policy, or remove contractor personnel who had unfavorable adjudications of their background investigations. We also found that administrative account management needed improvement.

[36] OMB Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management* (May 2019).
[37] 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.
[38] 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).

Contractor Confidentiality Agreements Not Consistently Maintained

The FDIC's Acquisition Policy Manual (APM) 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[39] prior to receiving or collecting sensitive FDIC information. 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. 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.

The purpose of executing Confidentiality Agreements is to inform contractor personnel of their obligations regarding the proper handling and safeguarding of sensitive information, and to hold accountable individuals who fail to meet those obligations. 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 information. Absent signed Confidentiality Agreements, the FDIC is at increased the risk of an unauthorized disclosure of sensitive information.

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 January 2006, the OIG reported that the FDIC did not maintain signed Confidentiality Agreements for 12 of 13 contracts reviewed.[40] In September 2008, the OIG reported that the FDIC did not maintain Confidentiality Agreements for 14 of 46 contractor personnel reviewed.[41] In October 2012, the OIG reported that the FDIC did not consistently execute and maintain Confidentiality Agreements for contractor and subcontractor personnel.[42] In September 2017, the OIG reported that the FDIC could not locate signed confidentiality agreements for 36 of the 48 contractor personnel.[43]

---

[39] FDIC Form 3700/46A, *Confidentiality Agreement*.
[40] FDIC OIG Report, *FDIC Safeguards Over Personal Employee Information* (Report No. EVAL-06-005, January 2006).
[41] FDIC OIG Report, *Protection of Resolution and Receivership Data Managed or Maintained by an FDIC* Contractor (Report No. AUD-08-015, September 2008).
[42] 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).
[43] FDIC OIG Report, *Controls over Separating Personnel's Access to Sensitive Information* (Report No. EVAL-17-007, September 2017).

Contractors with Unfavorable Background Investigations Not Always Removed

The FDIC has established policy and procedures to help ensure contractors and contractor personnel meet the FDIC's minimum standards of integrity and fitness and requirements for security eligibility and suitability.[44] The policy and procedures include requirements for performing preliminary security checks and ordering background investigations of contractor personnel with long-term access to FDIC facilities, systems, or sensitive information.[45] After completing a background investigation, the FDIC makes a final determination (adjudication) regarding the individual's suitability for employment. If the FDIC determines that an adjudication is unfavorable, the FDIC may remove the individual's access to FDIC systems or facilities, and notify the contractor to replace the individual on the contract.

We noted five instances in which contractor employees working for the FDIC had received an unfavorable adjudication of their background investigation, but the FDIC had not removed these individuals. These five exceptions were brought the attention of the FDIC during our audit, and the FDIC subsequently removed all five contractor employees.

Two of the five contractor employees worked as IT Administrators—positions of high trust in the FDIC's IT environment. The FDIC grants IT Administrators special network and system accounts called Administrative Accounts. These Administrative Accounts have elevated access privileges that IT Administrators use to create new accounts, change system configuration settings, and bypass system controls to perform troubleshooting activities. According to CIOO Policy 14-005, *Policy on Restricting Administrative Access to both Servers and Workstations* (June 2016), a compromise of an Administrative Account "poses a significant risk to the FDIC environment." By not removing the two IT Administrators immediately after their unfavorable adjudications, the FDIC was exposed to an increased risk of an insider threat or security incident.

Administrative Account Management Needed Improvement

The effective implementation of identity and access management controls are particularly important for Administrative Accounts within networks and information systems. As previously stated, 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.

---

[44] FDIC Directive 1610.2, *Personnel Security and Suitability Program for Contractors and Contractor Personnel (*January 2020), and FDIC *Personnel Security Procedures Guide for Contracting Officers and Oversight Managers*.

[45] Preliminary security checks consist of such things as fingerprint criminal records checks and reviews of personnel security questionnaires and credit reports. The FDIC permits contractor personnel to begin work and access systems and buildings after they have cleared preliminary checks, but before the completion of a background investigation. Background investigations consist (at a minimum) of a National Agency Check with Inquiries, which is a search of Federal investigative databases maintained by the Federal Bureau of Investigation and other Federal agencies, together with written inquiries of employers, educational institutions, law enforcement agencies, and references. The purpose of a background investigation is to gather enough information to determine whether an individual is reliable, trustworthy, of good conduct and character, and loyal to the United States.

As of August 26, 2020, we identified 14 open POA&Ms in CSAM that related to weaknesses in the FDIC's management of Administrative Accounts. Five of these 14 POA&Ms had an estimated completion date that was past due. According to these POA&Ms, the FDIC had not:

- [redacted];
- [redacted]
- [redacted]; or
- [redacted]

In addition to the weaknesses identified above, we have reported weaknesses related to Administrative Account management in each of our FISMA audit reports issued since 2017. In addition, 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.[47] The OIG also noted in its report that some [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 identified more than 1,500 instances in which: [redacted] 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.

Recommendation

We recommend that the CIO:

4. Assess the effectiveness of the FDIC's controls for managing Administrative Accounts and implement control improvements.

Data Protection and Privacy

Data Protection and Privacy involves implementing a privacy program to properly collect, safeguard, use, maintain, share, and dispose of PII. Organizations must consider the protection of PII over its

[46] Local Administrative Accounts are different from network accounts in that local Administrative Accounts control access to a single, physical IT device, such as a firewall. When an individual logs into the device using a local account, the IT device checks its own list of User IDs and passwords stored locally on the device to see if the individual is permitted access. This differs from a network account that uses a central security service, such as the Microsoft Active Directory (Active Directory), to identify and authenticate individuals.

[47] FDIC OIG Report, *Preventing and Detecting Cyber Threats* (Report No. AUD-19-005, May 2019). The report contained 10 recommendations. As of March 19, 2020, the FDIC OIG closed all 10 recommendations.

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 6: Maturity Rating – Data Protection and Privacy

The FDIC is operating at a Maturity Level 2 (*Defined*) 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,[48] 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)[49] 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.[50]

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,[51] Privacy Program Plan, and Breach Response Plan. However, as described below, the FDIC had not yet completed action to address a number of weaknesses in its Privacy Program identified by the FDIC OIG in an audit report issued in December 2019.[52] In addition, the FDIC had not yet completed action to address a recommendation issued 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.

---

[48] 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.

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

[50] 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.

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

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

Privacy Control Weaknesses Not Fully Addressed

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.

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[53] 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)[54] 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,[55] including implementing the Document Labeling initiative[56] intended to identify, categorize, label, and protect PII and sensitive information; and
- Ensure that Privacy Impact Assessments 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 Privacy Impact Assessments reduced transparency regarding the FDIC's practices for handling and protecting PII.

---

[53] Privacy Act of 1974, 5 U.S.C § 522a; 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); Section 522 of the Consolidated Appropriations Act of 2005, Pub. L. No. 108-447, 118 Stat. 2809, amended by Consolidated Appropriations Act of 2008, Pub. L. No. 110-161, 121 Stat. 1844 (codified as amended at 42 U.S.C. § 2000ee-2).

[54] 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.

[55] 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.

[56] 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 implements the Document Labeling initiative, there is an increased risk that sensitive data will not be properly handled and safeguarded.

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 Privacy Impact Assessments. As of September 9, 2020, the FDIC had taken action to close 2 of the OIG's 14 recommendations. Table 4 lists the FDIC's planned closure dates for the remaining 12 recommendations.

Table 4: Planned Closure Dates for Unimplemented OIG Privacy Program 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 4 Implement a PCM program to regularly assess the effectiveness of privacy controls.	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.	July 30, 2021
Recommendation 6 Establish a governance body or other governance mechanisms to assist the FDIC's Chief Records Officer with records management implementation and compliance.	March 29, 2021
Recommendation 7 Complete and implement the data protection program policy directive, data labeling guide, and associated job aids.	January 31, 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
Recommendation 9 Ensure that Divisions and Offices complete File Plans.	December 31, 2020
Recommendation 10 Perform annual evaluations of the Records and Information Management program.	December 31, 2020
Recommendation 11 Generate reports to monitor and audit compliance with the FDIC's records retention and disposition requirements.	December 31, 2020
Recommendation 12 Finalize and implement a records management framework for FDIC information systems that ensures compliance with records retention requirements.	December 31, 2020

Recommendation	Planned Closure Date
Recommendation 13 Revise and implement processes to ensure that Privacy Impact Assessments are completed and made available to the public prior to authorizing information systems containing PII to operate.	December 31, 2020
Recommendation 14 Revise and implement policy and/or processes to ensure Privacy Impact Assessments are periodically reviewed, updated, and removed from the FDIC's public website when systems are retired.	December 31, 2020

Source: Cotton & Company LLP's analysis of planned closure dates for privacy program recommendations in the FDIC's *Joint Audit Management Enterprise System* as of September 9, 2020.

Controls Over Sensitive Information Not Fully Implemented

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.[57] 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,[58] 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 access to the FDIC's internal network, included sensitive PII and information about employee performance and disciplinary actions.

[57] 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.

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

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.[59] In response to the first recommendation, the FDIC issued a global email 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 global email 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 conducted walkthroughs of its facilities in the Washington, D.C., metropolitan area and the Atlanta Regional Office between December 2019 and February 2020. The FDIC plans to conduct walkthroughs of its remaining five Regional Offices after it lifts mandatory telework for employees and contractors.

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. The FDIC explained that it needed additional time to establish a broader plan that leveraged internal access control systems to monitor network shared drive permissions. Accordingly, the second recommendation remains unimplemented.

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 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.[60]

Figure 7: Maturity Rating – Security Training

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

[59] These recommendations are listed in Appendix I as Recommendations 1 and 2 from the FISMA audit report issued in 2019.
[60] 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.

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 a week of employment, and annually thereafter, will have their access to network applications and systems revoked.

Our FISMA audit report issued in 2019 identified 29 network users who had not satisfied the FDIC's security and privacy awareness training requirement. However, these users retained access to the network. Prior to our FISMA report in 2019, the FDIC was not aware of the 29 users because the system used by the FDIC to monitor training compliance did not have complete information on users. Following last year's FISMA audit, the FDIC took steps to ensure that the system it uses to monitor user compliance with security and privacy awareness training requirements contained complete and accurate information. The FDIC also regularly captured and reported monthly metrics regarding the status of employee and contractor compliance with both security and privacy awareness training and specialized and role-based training.

The FDIC employed other means to promote security and privacy awareness within its workforce through various communication channels, such as global email messages and postings in FDIC facilities. 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 e-mails in an attempt to gather personal, financial, and other sensitive information from recipients, or to trick the recipients into downloading malicious software. Phishing emails often appear to come from well-known and trustworthy sources, such as financial institutions, government agencies, retailers, and popular Internet sites. OCISO collects and reports statistical information on the number of users who click on the links and attachments in the fake phishing emails.

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 8: Maturity Rating – Information Security Continuous Monitoring

The FDIC is operating at a Maturity Level 2 (*Defined*) in the *ISCM* domain.

The FDIC established and implemented policies and guidance to support the continuous monitoring of its information systems.[61] In addition, the CIOO implemented a security and privacy controls assessment program to conduct regularly scheduled tests of system security controls. The FDIC uses the results of these control assessments to evaluate the security risk posture of its information systems in support of ongoing security authorizations. Using dashboards, metrics, and other reporting mechanisms, the CIOO keeps Executive managers and other stakeholders informed of security risks. However, we found that the FDIC did not provide adequate security oversight and monitoring of its outsourced systems, or complete security control assessments for all of its cloud-based systems.

Oversight and Monitoring of Outsourced Systems Not Adequate

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 addition, NIST SP 800-171, Rev. 2,[62] provides organizations with recommended security requirements for protecting externally managed systems.

In our FISMA audit report issued in 2015,[63] 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 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.[64] In response to our recommendation, the CIOO took several actions, including the replacement of the OISPAM with a new

[61] FDIC Directive 1310.3, *Information Security Risk Management Program* (March 2020), and the *Information Security Risk Management Guide: Systems and Applications* (July 2018).
[62] NIST SP 800-171, Rev. 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (February 2020).
[63] FDIC OIG Report, *Audit of the FDIC's Information Security Program – 2015* (Report No. AUD-16-001, October 2015).
[64] This recommendation is listed in Appendix I as Recommendation 4 from the FISMA audit report issued in 2015.

Outsourced Solution Assessment Methodology (OSAM) in November 2018. The CIOO also developed a written plan to guide the transition of its outsourced service providers from the legacy OISPAM to the OSAM, and worked to implement the plan in 2019. The FDIC OIG closed the recommendation in April 2020.

In June 2020, during our field work for this 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 [65] defined in NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations* (December 2018). OMB Circular A-130 requires Federal agencies to follow the RMF. 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, these contractor systems were not subject to a proper risk assessment, authorization to operate, or ongoing monitoring as defined in the RMF.

Going forward, the OCISO plans to subject all FDIC systems, including those provided or supported by outsourced providers, to the RMF. The OCISO is implementing a three-phased approach to implement the RMF for all systems:

- **Phase 1** activities involve rescinding OSAM (completed); implementing the RMF for all new contracts that involve the procurement of contractor systems (ongoing); and issuing interim guidance for including security clauses in contracts involving contractor systems (not completed).
- **Phase 2** activities involve conducting a full review of the FDIC's current systems inventory and outsourced services covered by the legacy OSAM to ensure all systems are properly categorized and subject to the RMF (not started); integrating the RMF into the FDIC's procurement policies, processes, and guidance (not started); assessing and modifying, as appropriate, existing contracts to require the use of the RMF for systems (not started).
- **Phase 3** activities involve assessing the RMF process for contractor systems' need for continuous process improvement (not started).

If the FDIC does not consistently subject its outsourced systems 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.

Recommendation

We recommend that the CIO:

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

[65] 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.

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 on a frequency no less than annually. The *FDIC Security and Privacy Control Assessment (SCA) Methodology*[66] defines the FDIC's processes for assessing the effectiveness of controls in all FDIC-owned and/or operated information systems and cloud-based information systems. According to NIST SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*,[67] security and privacy control assessments are the principal vehicle used by agencies to verify that controls meet their stated goals and objectives.

The *SCA Methodology* requires security and privacy controls for cloud-based information systems to be assessed on a 3-year cycle, with at least some controls tested every year.[68] We reviewed the status of the FDIC's security and privacy control assessments for all 14 of the cloud-based systems the FDIC had authorized to operate as of April 1, 2020. These 14 systems provided critical IT services, such as [redacted]. As reflected in Table 5, the CIOO did not subject these 14 systems to annual security and privacy control assessments. In two cases, the FDIC had not completed annual control assessments for more than 3 years after the FDIC authorized the systems to operate.

Table 5: Status of Assessments of Cloud-Based Systems after Initial Authorization

Cloud System	Initial System Authorization Date	Status of Annual Assessment as of September 11, 2020
System 1	09/07/2016	Completed (July 9, 2020)
System 2	10/18/2016	Delayed*
System 3	02/22/2017	Planned
System 4	03/01/2017	Completed (June 17, 2020)
System 5	07/20/2017	Completed (July 6, 2020)
System 6	07/25/2017	Completed (September 2, 2020)
System 7	05/23/2018	In Progress
System 8	06/21/2018	In Progress
System 9	06/26/2018	Planned
System 10	03/08/2019	In Progress
System 11	03/28/2019	In Progress
System 12	03/29/2019	Planned
System 13	08/25/2019	Planned
System 14	09/24/2019	Planned

Source: Cotton & Company LLP's analysis of the FDIC's cloud-based systems inventory in CSAM as of April 1, 2020.
*Annual assessment delayed due to resource constraints.

[66] *FDIC Security and Privacy Control Assessment (SCA) Methodology*, Version 1.0 (April 2020).
[67] NIST SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, Rev. 4 (December 2014).
[68] In April 2020, the CIOO replaced its legacy methodology for conducting assessments of security controls with the *SCA Methodology*. The legacy methodology also required annual testing of security controls.

In September 2019, the FDIC created a POA&M to remediate the weakness that cloud-based systems were not subject to annual security and privacy control assessments. The POA&M recommended that all FDIC cloud-based information systems be added to the CIOO's annual security control assessment schedule. As of September 11, 2020, the CIOO had completed assessments for 4 of the 14 cloud-based systems, and had either initiated or planned assessments for the remaining 10 systems.

The FDIC uses the results of security and privacy control assessments to support a number of important risk management activities. Such activities include identifying security and privacy weaknesses in information systems and the IT environment; prioritizing risk mitigation activities; confirming the resolution of known security and privacy weaknesses; informing system authorization decisions; and supporting resource allocation decisions. Without annual control assessments, the FDIC may not identify and remediate security and privacy weaknesses in its cloud-based systems in a timely manner.

Recommendation

We recommend that the CIO:

6. Ensure that the FDIC's cloud-based information systems are subject to annual security and privacy control assessments.

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,[69] defines procedures for establishing and training 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 9: Maturity Rating – Incident Response

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

[69] NIST SP 800-61, Rev. 2 (August 2012).

The FDIC established policies and procedures for responding to computer security incidents;[70] 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.

We performed selected tests of compliance with the FDIC's incident response and reporting procedures and determined that the FDIC followed its procedures.

- We judgmentally selected 17 of 24 incidents recorded in the Combined Operational Risk, Security, Investigation, and Compliance Application (CORSICA)[71] between January 1, 2020, and May 15, 2020, and found that the FDIC:
    - Classified all 17 incidents consistent with the Attack Vectors Taxonomy defined by the United States Computer Emergency Readiness Team (US-CERT);[72] and
    - Resolved all 17 incidents within the timeframes prescribed in CSIRT's Standard Operating Procedures.
- We judgmentally selected 4 of 8 incidents (from a universe of 24 incidents) recorded in CORSICA with an Event Type of "Data Loss Prevention," and confirmed that the FDIC reported all 4 incidents to US-CERT within prescribed timeframes.

RECOVER

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

Contingency Planning

FISMA requires agencies to develop, document, and implement plans and procedures to ensure 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.

[70] 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).
[71] CORSICA is the FDIC's system of record for tracking and managing incidents.
[72] US-CERT is an organization within DHS that assists Federal civilian agencies with their incident handling efforts. FISMA requires Federal agencies to report security incidents to US-CERT, which analyzes the information to identify trends and indicators of attack across the Federal government. US-CERT has adopted a common set of terms and relationships to classify incidents based on a high-level set of attack vectors and descriptions developed from NIST SP 800-61, Rev. 2. All elements of Federal Government are required to use this common taxonomy to allow clear communication of incidents throughout the Federal Government and supported organizations.

Figure 10: Maturity Rating – Contingency Planning

The FDIC is operating at a Maturity Level 3 (*Consistently Implemented*) 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.[73] In addition, following our FISMA audit in 2019, the FDIC completed work on a multi-year effort to develop a new and expanded Backup Data Center designed to ensure IT systems and applications can be recovered within required timeframes. The new Backup Data Center also addressed a risk posed by the close geographic proximity of the legacy recovery facility to the FDIC's Primary Data Center.[74] Further, the new Backup Data Center includes enhanced security capabilities that will help ensure that security operations and other key security functions can be carried out without interruption in the event of a failure or other contingency at the Primary Data Center.

Contingency Planning Policy Needed to be Updated

FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, states that policies and procedures play an important role in the effective implementation of enterprise-wide information security programs within the Federal government. According to FIPS Publication 200, agencies must develop and promulgate documented policies and procedures governing the minimum security requirements set forth in the standard. Such minimum security requirements include contingency planning. Further, NIST SP 800-53, Rev. 4, recommends that agencies establish a contingency planning policy for their information systems, and review and update the policy to keep it current.

We reviewed FDIC Directive 1360.13, *Information Technology Contingency Planning* (May 2013), and found that it was outdated. For example, Directive 1360.13:

- Stated that "all mission critical systems [must] be recovered and available for use within [redacted] hours of a declared emergency." However, the [redacted] hour recovery timeframe is not consistent with the recovery timeframes in the FDIC's *2017-18 Business Process Analysis (BPA)/Business Impact Analysis (BIA) Final Report* (August 2018) (BPA/BIA Report). The BPA/BIA Report defines

[73] Such policies and procedures included FDIC Directives 1360.13, *Information Technology Contingency Planning* (May 2013); 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 DCOM and Windows Servers, and contingency plans for IT systems and applications that support mission-essential functions, such as the CAS and ALIS.

[74] NIST SP 800-34, Rev. 1, recommends that organizations identify an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards, such as environmental disasters (hurricanes, floods, and earthquakes) and man-made hazards (war or power grid failures). The FDIC's legacy recovery facility was about 25 miles from the FDIC's Primary Data Center. As a result, both computing centers were subject to similar natural, environmental, or man-made hazards.

varying "maximum tolerable downtimes" of [redacted], and [redacted] hours for mission-essential and mission-critical systems and applications.

- Referenced OMB policy and NIST SPs that have been withdrawn or superseded in recent years.
- Assigned various responsibilities to former the Information Security and Privacy Staff, which the FDIC renamed and reorganized into the OCISO in August 2017.
- Did not reflect changes to the FDIC's Emergency Preparedness Program and Continuity of Operations Program introduced in FDIC Directives 1500.5, *Emergency Preparedness Program* (November 2019), and 1500.6, *Continuity of Operations (COOP) Program* (November 2019).

CIOO personnel informed us that they were aware FDIC Directive 1360.13 was out-of-date, and had drafted revisions to the Directive. However, these revisions had not yet been approved or published by FDIC management.

NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, Rev. 1, states that effective contingency planning begins with the development of an organization contingency planning policy. Up-to-date policies are important because they communicate management's expectations, establish accountability, and serve as a basis for training staff on their duties and responsibilities. Without a current contingency planning policy, employees and contractor personnel may not implement contingency planning practices in a proper, consistent, or disciplined manner. Further, the FDIC is dependent on the knowledge and experience of a limited number of key staff, which exposes the FDIC to operational risk associated with workforce staffing changes. For example, if a key staff member were to depart the FDIC unexpectedly, the lack of a current policy could hamper the FDIC's ability to efficiently and effectively recover its IT systems and applications during an emergency.

Recommendation

We recommend that the CIO:

7. Update FDIC's directive(s) related to contingency planning to reflect current business processes, requirements, and government-wide security policy and guidance.

Testing of Contingency Plans Can Be Improved

In October 2019, the CIOO completed the first full test of its IT contingency plans following the implementation of the new Backup Data Center. The CIOO conducted the test during the same weekend that the FDIC's Division of Administration shut down power at the Primary Data Center to upgrade electrical and cooling equipment. The CIOO determined that testing its IT contingency plans when power at the Primary Data Center was shut down would validate whether the Backup Data Center could maintain IT operations during an outage at the Primary Data Center.

The CIOO prepared an After Action Report[75] of the contingency plan test which stated that "[o]verall, this exercise completed successfully." The After Action Report identified 41 action items to strengthen

[75] *Fall 2019 Disaster Recovery Preparedness Exercise After Action Results* (December 2019).

IT contingency planning. Such action items included: implementing improved redundancy for certain IT infrastructure and security services, including [redacted].

Because of the complexities involved in conducting an IT contingency plan test and the potential risk it poses of an IT service interruption, the CIOO conducted IT contingency plan tests over weekends when there was limited business activity. In addition, IT contingency plan tests were scheduled in advance, and application project managers and other key personnel held meetings to plan logistics and key activities and tasks to be conducting during the tests. However, the effectiveness of the CIOO's IT contingency plan testing could be improved if the CIOO incorporated additional scenarios into the testing.

NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities* (September 2006), recommends that organizations conduct contingency plan testing in a manner that resembles an operational environment as much as possible. [redacted] the FDIC experienced an unexpected drop in water pressure at its Primary Data Center [redacted]. According to a CIOO Awareness Report, [redacted], the drop in water pressure caused the cooling systems that provide air conditioning to the Primary Data Center to lose efficiency and caused the temperature in the Primary Data Center to rise. The CIOO Awareness Report stated that without adequate water pressure, the cooling systems would eventually stop working, making the Primary Data Center too hot for the computer equipment to continue operating.

In response to the rising temperature in the Primary Data Center, CIOO staff decided to power down some of the network IT equipment to reduce heat output, and transferred certain IT systems and services to the Backup Data Center. Because this event was not planned, certain key staff were not present to execute fail-over procedures to the Backup Data Center. In one case, a junior technician incorrectly executed scripts that inadvertently caused servers in the production environment to shut down. Based on the lessons learned from this event, the CIOO updated its IT contingency planning procedures to better describe the tasks needed to perform recovery operations. The CIOO should improve the effectiveness of its IT contingency plan testing by incorporating additional "real world" scenarios. Such scenarios could include:

- Removing one or more key personnel from future contingency plan test exercises to assess the associated impact on recovery efforts.
- Incorporating various scenarios into contingency plan testing, such as a malicious cyber security attack or a fire at the Primary Data Center that renders one or more critical IT services unavailable.
- Conducting unannounced testing.
- Stress-testing IT systems and applications following a fail-over to the Backup Data Center to mimic significant business activity that may occur during a recovery effort, such as a bank closing.

Adopting additional scenarios may identify new operational or process-related issues that need to be addressed. Identifying and addressing these issues would further the effectiveness and maturity of the FDIC's IT contingency planning capabilities.

Recommendation

We recommend that the CIO:

8. Incorporate additional scenarios involving operational challenges into the FDIC's IT contingency plan testing exercises.

CONCLUSION

The FDIC established a number of information security program controls and practices consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines. However, based on the results of our audit work and the application of the IG FISMA Reporting Metrics, we determined that the FDIC's information security program is operating at a Maturity Level 3 (*Consistently Implemented*). Our report contains eight new recommendations that, together with our prior-year recommendations, other 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 eight recommendations are as follows:

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.
2. Implement control improvements to prevent the unauthorized installation of software on the FDIC network.
3. Remediate incomplete and out-of-date baseline configurations.
4. Assess the effectiveness of the FDIC's controls for managing Administrative Accounts and implement control improvements.
5. Implement a process to ensure that all outsourced information systems are subject to the NIST Risk Management Framework as prescribed by OMB policy.
6. Ensure that the FDIC's cloud-based information systems are subject to annual security and privacy control assessments.
7. Update FDIC's directive(s) related to contingency planning to reflect current business processes, requirements, and government-wide security policy and guidance.
8. Incorporate additional scenarios involving operational challenges into the FDIC's IT contingency plan testing exercises.

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 2015, 2016, 2017, 2018, and 2019.

Recommendation	Status
Report Issued in 2015, Recommendation 4 Assess the Information Security Manager (ISM) *Outsourced Information Service Provider Assessment Methodology* processes supporting information service provider assessments to determine and implement any needed improvements to ensure timely completion of assessments.	Closed
Report Issued in 2016, Recommendation 5 Review existing resource commitments and priorities for addressing DCOM POA&Ms, and take appropriate steps to ensure they are addressed in a timely manner.	Open
Report Issued in 2017, Recommendation 4 Develop a method and strategy for use by FDIC Divisions and Offices in the classification of risk ratings and risk profiles of applications and systems.	Closed
Report Issued in 2017, Recommendation 5 Develop and communicate the FDIC's information security risk tolerance level and risk profile used to prioritize risk mitigation activities.	Closed
Report Issued in 2017, Recommendation 9 Ensure that the improvements to the FDIC's patch management process result in systems being patched in accordance with FDIC's patch management policy and National Institute of Standards and Technology (NIST) recommended practices.	Closed
Report Issued in 2017, Recommendation 10 Review and enhance the FDIC's vulnerability scanning processes to ensure that issues associated with conducting credentialed scans are resolved in a timely manner.	Closed
Report Issued in 2017, Recommendation 15 Develop an approach and implementation procedures for evaluating risk associated with known security weaknesses and vulnerabilities to ensure they collectively remain within established risk tolerance levels.	Closed
Report Issued in 2018, Recommendation 2 Develop and implement procedures that define how the results of manual configuration reviews are used to assess compliance with approved baseline configurations.	Closed
Report Issued in 2018, Recommendation 4 Develop and implement a process to ensure that vulnerabilities resulting from patches that have not been installed within required timeframes are tracked and reported to senior management.	Closed
Report Issued in 2019, Recommendation 1 Reinforce to employees and contractor personnel the importance of properly safeguarding sensitive electronic and hardcopy information.	Closed
Report Issued in 2019, Recommendation 2 Monitor employee and contractor compliance with policy requirements for properly safeguarding sensitive electronic and hardcopy information.	Open

Recommendation	Status
Report Issued in 2019, Recommendation 3 Implement controls that ensure FDICLearn maintains accurate and complete information regarding user compliance with the FDIC's security and privacy awareness training requirement.	Closed

APPENDIX II – LIST OF ACRONYMS

Acronym	Description
ALIS	Advanced Legal Information System
APM	Acquisition Policy Manual
AR	Acceptance of Risk
BIA	Business Impact Analysis
BPA	Business Process Analysis
CAS	Claims Administration System
CDO	Chief Data Officer
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CIOO	Chief Information Officer Organization
CISO	Chief Information Security Officer
COO	Chief Operating Officer
COOP	Continuity of Operations
CORSICA	Combined Operational Risk, Security, Investigation, and Compliance Application
CPO	Chief Privacy Officer
CRO	Chief Risk Officer
CSAM	Cyber Security Assessment and Management
CSIRT	Computer Security Incident Response Team
DCOM	Data Communications
DHS	Department of Homeland Security
DIT	Division of Information Technology
EA	Enterprise Architecture
ERM	Enterprise Risk Management
FDIC	Federal Deposit Insurance Corporation
FedRAMP	Federal Risk and Authorization Management Program
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAO	Government Accountability Office
HSPD-12	Homeland Security Presidential Directive 12
ICAM	Identity, Credential, and Access Management
IG	Inspector General
ISCM	Information Security Continuous Monitoring
ISM	Information Security Manager
IT	Information Technology
ITRAC	IT Risk Advisory Committee
NIST	National Institute of Standards and Technology

OCISO	Office of Chief Information Security Officer
ODNI	Office of the Director of National Intelligence
OIG	Office of Inspector General
OISPAM	Outsourced Information Service Provider Assessment Methodology
OMB	Office of Management and Budget
OPM	Office of Personnel Management
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
RMF	Risk Management Framework
RMIC	Risk Management and Internal Controls
SAOP	Senior Agency Official for Privacy
SAR	Suspicious Activity Reports
SCA	Security and Privacy Control Assessment
SEATAB	Security and Enterprise Architecture Technical Advisory Board
SP	Special Publication
TIC	Trusted Internet Connection
US-CERT	United States Computer Emergency Readiness Team

Part II

☆☆☆☆☆☆☆☆

FDIC Comments and OIG Evaluation

FDIC Comments and OIG Evaluation

The FDIC's Chief Information Officer (CIO) and Chief Information Security Officer (CISO) provided a written response, dated October 21, 2020, to a draft of the report. The response is presented in its entirety beginning on page II-2. In the response, CIO and CISO concurred with all eight 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-8.

The response also included management's views on three recommendations made in a prior OIG evaluation report on the FDIC's implementation of Enterprise Risk Management.[1] These three recommendations, which were based on government and industry-recognized best practices, remain unresolved because the FDIC's planned corrective actions did not satisfy the intent of the recommendations. We are seeking resolution of these recommendations through the FDIC's evaluation follow-up process.

[1] FDIC OIG Report, *The FDIC's Implementation of Enterprise Risk Management* (Report No. EVAL-20-005, July 2020).

FDIC
Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226-3500
Office of the Chief Information Officer

October 21, 2020

TO: Mark F. Mulholland
Assistant Inspector General for Audits

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

Zachary N. Brown **/Signed/**
Chief Information Security Officer

SUBJECT: Management Response to the Draft Audit Report Entitled *Audit of the FDIC's Information Security Program–2020* (Assignment No. 2020-007)

Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report on the *Audit of the FDIC's Information Security Program – 2020 issued* on October 08, 2020. The FDIC recognizes the objective of the annual OIG FISMA audit is to evaluate and determine the effectiveness of the Corporation's information security policies, procedures, and practices. We appreciate the OIG's assessment, findings, and recognition of several improvements made in the FDIC's information security program during the past year. For example, we appreciate the OIG's acknowledgement that the CIO Organization (CIOO) completed actions to close 10 of 12 recommendations from prior year FISMA audit reports; developed new or revised procedures in key security control areas such as system authorizations, patch management, and security and privacy control assessments; and completed work on the new Backup Data Center to enhance the resiliency and availability of IT systems and applications supporting mission-essential business functions.

In its report, the OIG/Cotton & Company Inc. (C&C) audit team made eight recommendations to the Chief Information Officer (CIO). As a result of the audit and subsequent discussions, the CIOO concurs with each of the eight recommendations. The information security issues that are identified in the report represent opportunities for the FDIC to better ensure risk management and configuration management controls are applied consistent with OMB policy, NIST guidance, and internal 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 strengthen. Regarding risk management, the OIG FISMA report rated the Risk Management function area, which includes FISMA metrics related to Enterprise Risk Management (ERM), as "Consistently Implemented." The FDIC does not dispute that rating with respect to the ERM FISMA metrics, and acknowledges that while the agency has made substantial progress, it can do more to mature and refine the ERM program. However, report references to OIG recommendations from a recent ERM evaluation with which the FDIC disagreed, require additional context. The FDIC rarely disagrees with audit

recommendations and held extensive discussions with OIG to attempt to reach agreement on recommendation language. The primary disagreement involves the appropriate role of the FDIC's Operating Committee. The FDIC designated the Operating Committee as the agency's Risk Management Council. The FDIC disagreed with the OIG's recommendation because it was inconsistent with the FDIC's operating model of decentralized decision-making. However, the FDIC stated it would assess whether ERM procedures needed to be updated to better explain the Operating Committee's role. The FDIC also contended that the criteria the OIG used in the evaluation to support its position was based on best practices that afford the FDIC considerable discretion.

The FISMA report also noted two recommendations from the ERM Report related to the FDIC Board of Directors that the OIG considers unresolved. These recommendations involved defining Board roles and responsibilities with respect to ERM and developing and implementing ERM communication protocols to the Board. The FDIC agreed to have the Board adopt the Risk Appetite statement annually and to memorialize in ERM procedures protocols for communicating ERM information semiannually to the FDIC Board through the FDIC's Audit Committee. The Audit Committee is a standing committee established by the Board with two Board members and a Chairman's designee. The FDIC will continue to work with the OIG to resolve these recommendations.

The CIOO continuously strives to improve our IT processes and enhance our information security risk posture through various activities that have allowed us to identify control gaps, and to take appropriate actions to remediate risk. We believe that actions we have completed, are currently pursuing, along with actions we will take in response to the 2020 FISMA report, will further improve and strengthen the FDIC's information security program and posture. The FDIC is committed to continuing its efforts to strengthen the overall cybersecurity of its networks, systems, and data, as reflected in the draft report.

MANAGEMENT RESPONSE

Recommendations 1 –

We recommend that the CIO:

1. Ensure that risk acceptance decisions are re-assessed in accordance with FDIC guidance to determine whether they remain valid and are at an acceptable level.

Management Decision: Concur

Corrective Action:

The FDIC will ensure that risk acceptances are reviewed and approved in accordance with FDIC guidance. Additionally, the FDIC will report risk acceptance metrics to management periodically to enable management to make informed decisions about whether or not they remain within acceptable risk tolerance levels.

Estimated Completion Date: 1/31/2021

Recommendations 2 –

We recommend that the CIO:

2. Implement control improvements to prevent the unauthorized installation of software on the FDIC network.

Management Decision: Concur

Corrective Action:

The FDIC will develop controls through processes and procedures to ensure Virtual Desktop Interface (VDI) gold templates are updated with only FDIC approved software. Compliance scans will also be conducted to ensure gold templates do not contain unauthorized software.

Estimated Completion Date: 6/30/2021

Recommendation 3 –

We recommend that the CIO:

3. Remediate incomplete and out-of-date baseline configurations.

Management Decision: Concur

Corrective Action:

The FDIC will remediate all out-of-date baseline configuration POA&Ms identified by the OIG during the audit.

Estimated Completion Date: 6/30/2021

Recommendation 4 –

We recommend that the CIO:

4. Assess the effectiveness of the FDIC's controls for managing Administrative Accounts and implement control improvements.

Management Decision: Concur

Corrective Action:

The FDIC will conduct a risk assessment to determine the root cause issues for open POA&Ms associated with the AC-2 control area and implement control improvements as needed.

Estimated Completion Date: 6/30/2021

Recommendation 5 –

We recommend that the CIO:

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

Management Decision: Concur

Corrective Action:

The FDIC will draft new security and privacy contract language and update the prescriptions for several existing security and privacy clauses, including the clause requiring NIST SP 800-171 controls, to ensure contractor systems and/or services are assessed and authorized pursuant to the NIST Risk Management Framework (NIST SP 800-37). Additionally, the OCISO will be embedding itself earlier in the acquisition process in order to ensure the proper implementation of privacy and security requirements. In doing so, OCISO is directly reviewing each Checklist for Information Security and Privacy Provisions/Clauses (Checklist), which DOA/ASB uses to document the provisions/clauses required to be included in each contract, to make certain there is consistent implementation of privacy and security requirements as its relates to contractor systems and/or services. By ensuring that all outsourced service providers (contractors) are subject to NIST 800-37, the FDIC will require contractors operating contractor IT systems to obtain an Authority to Operate signed by the FDIC Authorizing Official, granted through the System Security Authorization (SSA) process. This includes SSA process documentation, an independent assessment, support of completion of privacy

compliance documentation, authorization to operate, and continuous monitoring/ongoing assessment.

Estimated Completion Date: 12/31/2021

Recommendation 6 –

We recommend that the CIO:

6. Ensure that the FDIC's cloud-based information systems are subject to annual security and privacy control assessments.

Management Decision: Concur

Corrective Action:

The FDIC will complete security control assessments for cloud based systems annually.

Estimated Completion Date: 12/31/2021

Recommendation 7 –

We recommend that the CIO:

7. Update FDIC's directive(s) related to contingency planning to reflect current business processes, requirements, and government-wide security policy and guidance.

Management Decision: Concur

Corrective Action:

The FDIC will update the directive related to contingency planning to reflect current business processes, requirements, and government-wide security policy and guidance

Estimated Completion Date: 6/30/2021

Recommendation 8 –

We recommend that the CIO:

8. Incorporate additional scenarios involving operational challenges into the FDIC's IT contingency plan testing exercises.

Management Decision: Concur

Corrective Action:

The FDIC will incorporate additional scenarios involving operational challenges into the FDIC's IT contingency plan testing exercises.

Estimated Completion Date: 12/30/2020

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

cc: E. Marshall Gentry, Deputy Director, DOF, Risk Management and Internal Controls Branch
Greg S. Kempic, DOF, Risk Management and Internal Controls Branch
Jennah Mathieson, Deputy Director, Enterprise Strategies Branch

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 ensure that risk acceptances are reviewed and approved in accordance with FDIC guidance. Additionally, the FDIC will report risk acceptance metrics to management periodically to enable management to make informed decisions about whether they remain within acceptable tolerance levels.	January 31, 2021	$0	Yes	Open
2	The FDIC will develop controls through processes and procedures to ensure Virtual Desktop Interface gold templates are updated with only FDIC approved software. The FDIC will also conduct compliance scans to ensure gold templates do not contain unauthorized software.	June 30, 2021	$0	Yes	Open
3	The FDIC will remediate all out-of-date baseline configuration POA&Ms identified by the OIG during the audit.	June 30, 2021	$0	Yes	Open
4	The FDIC will conduct a risk assessment to determine the root causes of open POA&Ms associated with the information system Account Management (Access Control-2) control area defined in NIST SP 800-53, Rev. 4, and implement control improvements as needed.	June 30, 2021	$0	Yes	Open
5	The FDIC will draft new security and privacy contract language, and update existing security and privacy clauses, to ensure contractor systems and/or services are assessed and authorized pursuant to the NIST SP 800-37. Additionally, the OCISO will engage earlier in the acquisition process to ensure the proper implementation of security and privacy requirements for contractor systems and/or services.	December 31, 2021	$0	Yes	Open
6	The FDIC will complete security control assessments for cloud-based systems annually.	December 31, 2021	$0	Yes	Open
7	The FDIC will update the directive related to contingency planning to reflect current business processes, requirements, and government-wide	June 30, 2021	$0	Yes	Open

	security policy and guidance.				
8	The FDIC will incorporate additional scenarios involving operational challenges into the FDIC's IT contingency plan testing exercises.	December 30, 2020	$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 partially concurs or does not concur with the recommendation, but alternative action meets the intent of the recommendation.
3. Management agrees to the OIG monetary benefits, or a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

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

Federal Deposit Insurance Corporation
Office of Inspector General

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

(703) 562-2035

★★★★★★

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

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