# The FDIC's Information Security Program–2019

October 2019 AUD-20-001

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.**

Integrity☆Independence☆Accuracy☆Objectivity☆Accountability

Executive Summary

# The FDIC's Information Security Program–2019

The Federal Information Security Modernization Act of 2014 (FISMA) 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 reporting metrics (referred to as the "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. The five maturity level ratings are (1) Ad Hoc, (2) Defined, (3) Consistently Implemented, (4) Managed and Measurable, and (5) Optimized.

## 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 below a Maturity Level 4 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.

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. The FDIC also took or was working to take steps to strengthen its information security program controls following the FISMA audit conducted in 2018. For example, the FDIC developed new or revised policies and procedures in key security control areas; issued a new agency-wide

Identity, Credential, and Access Management Program Strategy and supporting architecture in response to revised Federal requirements; and made substantial progress towards completing a new backup data center to help ensure that information technology (IT) systems and applications supporting mission-essential functions can be recovered within targeted timeframes.

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

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.  We have identified the six highest risk weaknesses and described them below.

**Risk Management (Identify)**.  OMB and NIST policies and guidance help agencies implement Enterprise Risk Management (ERM) programs to manage the risks agencies face.

The FDIC took steps towards aligning its risk management activities with OMB policy and NIST guidance following our FISMA audit in 2018, including issuing an ERM policy and procedure, establishing a dedicated ERM Unit, and issuing a Risk Appetite statement.  However, the FDIC had not yet completed an inventory of risks facing the FDIC, or a Risk Profile to help manage and prioritize risk mitigation activities.  The FDIC had also not completed actions to address two recommendations made in our FISMA audit report issued in 2017 to develop a method and strategy to classify risk ratings and risk profiles of applications and systems, and develop and communicate the FDIC's information security Risk Tolerance level and Risk Profile.  The FDIC intends to complete actions to address these recommendations by January 2020.

**Network Firewalls (Protect)**.  According to NIST guidance, firewalls are essential devices or programs that help organizations protect their networks and information systems from hostile attacks, break-ins, and malicious software.  The FDIC deploys firewalls at both the perimeter and interior of its network.  These firewalls control the flow of inbound traffic from the Internet through the use of "ingress" rules that inspect traffic and permit or deny requests for access to FDIC systems.  The firewalls also control the type of traffic allowed to flow out of the network using "egress" rules.  Therefore, the FDIC's firewalls are only as effective as the rules that the FDIC defines for them.

In May 2019, we issued an audit report finding that many FDIC network firewall rules lacked a documented justification and the majority of rules were unnecessary. Several factors contributed to these weaknesses, including an inadequate firewall policy and supporting procedures, and an ineffective process for periodically reviewing firewall rules to ensure their continued need. Unnecessary firewall rules pose a security risk [redacted]. The FDIC took significant steps to address the network firewall weaknesses we identified. However, the FDIC had not yet completed actions to document all existing network firewall rules with an approval and mission/business need, including the duration of that need, or implemented a firewall policy consistent with NIST guidance. The FDIC intends to complete these actions by January 2020.

**Privileged Account Management (Protect).** The FDIC assigns certain network users "administrative accounts" that have privileged access to systems and network IT resources to perform maintenance and IT troubleshooting activities. The FDIC must carefully control and monitor administrative accounts because hackers and other adversaries often target them to perform malicious activity, such as exfiltrating sensitive information.

In May 2019, we issued an audit report finding that the FDIC did not always require administrators to uniquely identify and authenticate when they accessed network firewalls. In addition, we found instances in which [redacted]. These vulnerabilities exposed the network firewalls to increased risk of unauthorized access or malicious activity. Further, in November 2018, a consulting firm engaged by the FDIC to assess security controls on the internal network found [redacted].

**Protection of Sensitive Information (Protect).** Federal law, 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. The FDIC did not adequately control access to sensitive information stored on its internal network or in its facilities, including sensitive personally identifiable information, such as employee names, addresses, and Social Security Numbers; confidential bank examination information; financial investigation case files; procurement sensitive information; attorney-client privileged information; suspicious activity reports; and employee administrative actions. We conducted unannounced walkthroughs of selected FDIC facilities and identified significant quantities of sensitive hard copy information stored in unlocked filing cabinets and boxes in building hallways. We also identified instances in which sensitive information stored on internal network shared drives was not restricted to authorized users.

**Security and Privacy Awareness Training (Protect).** FDIC policy requires employees and contractor personnel with network access to complete security and privacy awareness training within one week of employment, and annually thereafter. FDIC policy states that users who fail to comply with this requirement must have their network access revoked. We identified 29 network users who did not satisfy the FDIC's awareness training requirement, but still had access to the network. We found that the FDIC was not aware of the 29 users because the system used to monitor training compliance did not track all users required to take the annual security and privacy awareness training.

**Security Control Assessments (Detect).** FISMA requires agencies to test and evaluate information security controls periodically in order to ensure that they are effective. The FDIC assessed its security controls following a risk-based schedule as recommended by NIST. However, in January 2019, we reported instances that occurred in 2016 and 2017 in which security control assessors did not test the implementation of security controls, when warranted. Instead, assessors relied on narrative descriptions of controls in FDIC policies, procedures, and system security plans and/or interviews of FDIC or contractor personnel. Without testing, assessors did not have a basis for concluding on the effectiveness of security controls.

## Recommendations

The FISMA report contains three new recommendations addressed to the Chief Information Officer that are intended to ensure (i) employees and contractor personnel properly safeguard sensitive electronic and hardcopy information and (ii) network users complete required security and privacy awareness training. The FDIC concurred with all three recommendations and planned to complete corrective actions by May 29, 2020. As described in the report, the FDIC was working to address an additional six recommendations from prior FISMA audit reports. These outstanding recommendations are intended to strengthen security controls in the areas of risk management, contactor-provided services, Plans of Action and Milestones, and vulnerability and compliance scanning. Further, at the close of our audit, we were reviewing the FDIC's actions to address three recommendations from prior FISMA audit reports to determine whether the actions were responsive.

# Contents

Part I

Part II

# Part I

☆☆☆☆☆☆☆☆

Report by Cotton & Company LLP

# THE FEDERAL DEPOSIT INSURANCE CORPORATION'S INFORMATION SECURITY PROGRAM – 2019

## AUDIT REPORT

## OCTOBER 23, 2019

Cotton& Company

Answers Questioned

Cotton & Company LLP
635 Slaters Lane
Alexandria, Virginia 22314
703.836.6701 | 703.836.0941, fax
lschwartz@cottoncpa.com | www.cottoncpa.com

# TABLE OF CONTENTS

Cotton & Company

Cotton & Company LLP
635 Slaters Lane
4th Floor
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 – 2019

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-15-G-0161-0008. Cotton & Company LLP performed the work from April through September 2019.

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,
Cotton & Company LLP

Loren Schwartz, CPA, CISSP, CISA
Partner, Information Assurance

# INTRODUCTION

According to the Office of Management and Budget (OMB), America's public and private networks remain top targets of malicious actors.[1] Every day, Federal agencies defend their information systems and data against cyberattacks. OMB reported that Federal agencies experienced 31,107 cybersecurity incidents during Fiscal Year (FY) 2018.[2] In addition to addressing a large number of cybersecurity incidents, Federal agencies also face cyber threats[3] that are increasingly sophisticated.

The Federal Deposit Insurance Corporation (FDIC) relies heavily on information systems to carry out its responsibilities of insuring deposits, supervising insured financial institutions, and resolving failed insured financial institutions. 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 in our Nation's financial system.

The Federal Information Security Modernization Act of 2014 (FISMA)[4] requires Federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. FISMA directs NIST to develop risk-based standards and guidelines to assist agencies in defining security requirements for their information and information systems. NIST 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;

[1] OMB, *Federal Information Security Modernization Act of 2014 Annual Report to Congress*, Fiscal Year 2018.
[2] OMB, *Federal Information Security Modernization Act of 2014 Annual Report to Congress*, Fiscal Year 2018.
[3] The National Institute of Standards and Technology (NIST) Special Publication 800-150, *Guide to Cyber Threat Information Sharing* (October 2016) defines the term, "cyber threat," as "any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service."
[4] 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.

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

The President's Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 2017),[5] 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 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, 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. 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our preliminary findings and conclusions with FDIC Office of Inspector General (OIG) officials and FDIC management officials throughout the 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, 2019 (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-19-02, *Fiscal Year*

[5] 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.

*2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, dated October 25, 2018, when planning and conducting our work.

- Assessed the maturity of the FDIC's information security program with respect to the metrics defined in DHS's document, entitled *Fiscal Year (FY) 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.3* (IG FISMA Reporting Metrics), dated April 9, 2019. The IG FISMA Reporting Metrics, which are discussed later, 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 service (listed below). Our analysis of these systems and the contractor service 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 FDIC's network information technology (IT) environment. DCOM also interfaces with 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 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.

  - *Regional Automated Document Distribution and Imaging System (RADD)*
    RADD is a document imaging, routing, and storage system. RADD contains sensitive information, including PII related to bank officers, employees, and customers; financial institution examination workpapers; reports of examination; loan records; bank correspondence; and other examination-related documentation, such as financial institution applications and supervisory actions. Various internal and external stakeholders use RADD to support bank supervisory activities.

  **Contractor Service**

  - *FDIC Business Data Services (FBDS)*
    FBDS contains records pertaining to financial institution failures. Such records include, for example, loan and deposit data, financial reports, email communications, file shares, suspicious activity reports, reports of examination, human resource records, and bank Board of Directors' minutes. Various internal and external stakeholders, including outside counsel, use FBDS to support critical activities, such as investigations, litigation, customer service, tax administration, research, and asset sales.

We selected the systems and the contractor service described above because they contain large quantities of sensitive information and support mission-essential functions, such as supervising insured financial institutions, managing failed financial institutions, and protecting depositors of insured financial institutions.  A disruption of these systems or service could impair the FDIC's ability to achieve its mission successfully.

As part of the audit, we considered the results of recent and ongoing audit and evaluation work conducted by the FDIC OIG and the Government Accountability Office (GAO), relating to the FDIC's information security program controls and practices.  Cotton & Company LLP conducted the audit at the FDIC's Virginia Square offices in Arlington, Virginia, from April through September 2019.  Except as noted in the report, our results are as of July 8, 2019.

## 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.

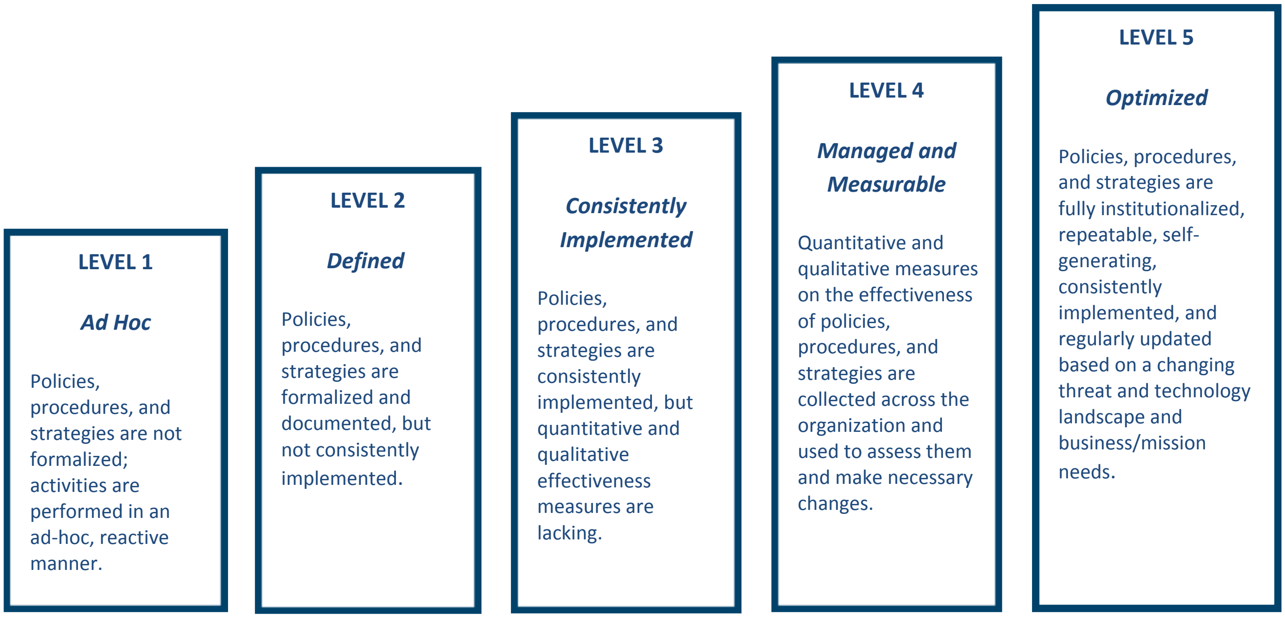
**Table 1:  Alignment of the NIST Cybersecurity Framework Function Areas with the IG FISMA Reporting Metric Domains**

| 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** |

Sources: 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 based on a maturity model spectrum. 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**



**LEVEL 1**

***Ad Hoc***

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

**LEVEL 2**

***Defined***

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

**LEVEL 3**

***Consistently Implemented***

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

**LEVEL 4**

***Managed and Measurable***

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

**LEVEL 5**

***Optimized***

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

Source: IG FISMA Reporting Metrics.

## Overview of the FDIC's Information Security Program

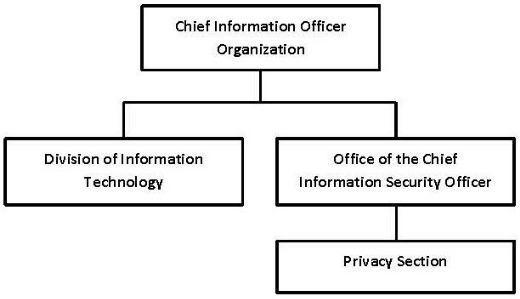
Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Agency heads are also responsible 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.dhs.gov/publication/fy19-fisma-documents.

The FDIC Chairman 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] 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 responsible for establishing and implementing a wide range of privacy and data protection policies and procedures pursuant to various legislative and policy requirements. 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 CIO and CISO coordinate with the Director, Division of Information Technology (DIT), who is responsible for managing the FDIC's IT functions. The Director, DIT, reports to the CIO.

The CISO oversees a group of security and privacy professionals within the Office of the CISO (OCISO), which is part of the CIO Organization (CIOO). The mission of the OCISO is to provide enterprise-wide information security and privacy programs that assure integrity, confidentiality, and availability of corporate information by proactively protecting IT assets. The FDIC has also designated a Privacy Program Manager position within OCISO's Privacy Section to oversee the FDIC's Privacy Program. Figure 2 illustrates the organizational structure of the CIOO.

**Figure 2: CIOO Structure**


Chief Information Officer Organization
Division of Information Technology
Office of the Chief Information Security Officer
Privacy Section

Source: Cotton & Company LLP analysis of the CIOO's Website.

FDIC Divisions and Offices also play an important role in securing information and information systems. The FDIC has Information Security Managers (ISMs) 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 corporate 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.

## 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

[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).

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

Source: Cotton & Company LLP's analysis of the FDIC's information security program controls and practices and 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 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 2018. For example, the FDIC:

- Developed new and revised security policies and procedures in areas such as Plans of Action and Milestones (POA&Ms); network firewalls; security patch management; breach response; systems interconnections; and risk management.
- Issued a new agency-wide Identity, Credential, and Access Management (ICAM) Program Strategy and supporting architecture to guide the implementation of ICAM activities and to help ensure alignment with revised Federal ICAM requirements.
- Made substantial progress toward completing a new backup data center intended to ensure that designated IT systems and applications supporting mission-essential FDIC functions can be recovered within targeted timeframes.

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

Below, we provide a brief description of the security control weaknesses that pose the highest risk of impacting the confidentiality, integrity, or availability of the FDIC's information systems and data. In addition, Appendix I contains the status of recommendations made in FISMA reports issued in prior years.

**Information Security Risk Management (Identify – Risk Management).** OMB and NIST policies and guidance help agencies implement Enterprise Risk Management (ERM) programs to effectively manage the risks agencies face in achieving their strategic objectives and arising from their activities and operations.

The FDIC took steps towards aligning its risk management activities with OMB policy and NIST guidance following our FISMA audit in 2018. Such steps included issuing an ERM policy and procedure, establishing a dedicated ERM Unit, and issuing a Risk Appetite statement.[8] However, the FDIC had not completed its Risk Inventory to manage and prioritize risk mitigation activities, or completed the Agency's Risk Profile.[9] The FDIC had also not completed actions to address two recommendations made in our FISMA audit report issued in 2017. These recommendations focused on (1) developing a method and strategy for use by Divisions and Offices in the classification of risk ratings and risk profiles of applications and systems and (2) developing and communicating the FDIC's information security Risk Tolerance level[10] and Risk Profile used to prioritize risk mitigation activities. The FDIC plans to complete actions to address these recommendations by January 2020. Completing the Risk Inventory and Risk Profile, and addressing these recommendations, will help ensure that the FDIC allocates its resources towards addressing risks with the most significant potential impact on achieving strategic objectives.

In addition, our report discusses a key information security risk facing the FDIC. In July 2019, the CIOO completed an IT Modernization Plan to address obsolete technologies within its IT environment that are becoming increasing fragile, unreliable, and costly to maintain. Modernizing the FDIC's IT environment will result in significant changes to how the CIOO delivers IT services and products, and the corresponding competencies and skills needed for its IT workforce. At the same time, the CIOO is working to re-compete one of the FDIC's largest contracts—the IT Infrastructure Support Contract 3 (ISC-3)—which covers a wide-range of IT services, including certain information security services. The ISC-3 contractors account for more than [redacted] percent of the CIOO's workforce. A re-compete of a large and complex contract such as the ISC-3 presents certain risks, such as the potential for a competing contractor to protest the FDIC's solicitation or award of the contract.[11] Such a protest would require the FDIC to expend resources to defend its procurement decisions, potentially delaying the acquisition of IT services and resulting in the loss of institutional knowledge should incumbent contractor personnel leave the FDIC to find other employment. The FDIC experienced such risks beginning in 2012, when the

[8] The FDIC defines Risk Appetite as a broad based amount of risk an organization is willing to accept in pursuit of its objectives.
[9] The FDIC defines a Risk Profile as a prioritized list of the most significant risks identified and assessed through the risk assessment process.
[10] The FDIC defines Risk Tolerance as the acceptable level of variance in performance relative to the achievement of objectives.
[11] Federal law provides mechanisms for contractors to "protest" (i.e., object to) contract solicitations and awards for failing to comply with Federal law. 31 U.S.C. § 3552. Such protests are referred to as "bid protests" and generally involve a contractor objecting to the conduct of a government agency in acquiring supplies and services for its direct use or benefit. Among other things, the challenged conduct can include violations of law or regulation in the way in which an agency solicits offers for a contract, cancels such a solicitation, awards a contract, or cancels a contract. See, e.g., 31 U.S.C. § 3551(1)(A)-(E).

former incumbent contractor for infrastructure services pursued bid protests that delayed the award of the contract.

Both OMB and the Federal IG community have identified the planning and acquisition for modernizing IT infrastructure and the recruitment and retention of a highly skilled cybersecurity workforce as a top challenge facing the Federal Government.[12] As the FDIC implements its IT Modernization Plan, it must give adequate consideration to information security, including the competencies and skills needed for its employees and contractors that provide security services. This is critical for ensuring the FDIC's information systems and data remain reliable, secure, and capable of supporting mission-essential functions.

**Network Firewalls (Protect – Configuration Management).** According to NIST, firewalls are essential devices or programs that help organizations protect their networks and information systems from hostile attacks, break-ins, and malicious software. Firewalls control access and network traffic permissions through the use of "rules."

In May 2019, the FDIC OIG reported a number of weaknesses that limited the effectiveness of the FDIC's network perimeter and interior firewalls.[13] According to the report, many firewall rules lacked a documented justification, and the majority of rules were unnecessary. Several factors contributed to these weaknesses, including an inadequate firewall policy and supporting procedures, and an ineffective process for periodically reviewing firewall rules to ensure their continued need. Unnecessary firewall rules pose a security risk [redacted] The FDIC took significant steps during our audit to address the network firewall-related weaknesses identified in the FDIC OIG's report. However, the FDIC had not yet completed actions to document all existing network firewall rules with an approval and mission/business need, including the duration of that need, and implement a firewall policy consistent with NIST guidance. The FDIC plans to complete these actions by January 2020.

**Privileged Account Management (Protect – Identity and Access Management).** The FDIC assigns "administrative accounts" to certain network users, who receive privileged (elevated) access to systems and network IT resources to perform maintenance and other types of necessary IT troubleshooting activities. Administrative accounts must be carefully controlled and monitored because hackers and other adversaries often target them to perform malicious activity, such as exfiltrating sensitive information.

In its report entitled *Preventing and Detecting Cyber Threats*, dated May 2019,[14] the FDIC OIG identified instances in which the FDIC did not always require administrators to uniquely identify and authenticate when they accessed network firewalls. The FDIC OIG's report also noted instances in which [redacted], which is prohibited by FDIC

[12] CIGIE Report, *Top Management and Performance Challenges Facing Multiple Federal Agencies* (April 2018) and OMB Memorandum M-16-15, *Federal Cybersecurity Workforce Strategy* (July 2016).
[13] OIG Report, *Preventing and Detecting Cyber Threats* (FDIC OIG AUD-19-005) (May 2019).
[14] FDIC OIG AUD-19-005.

policy. These vulnerabilities exposed the network firewalls to increased risk of unauthorized access and malicious activity.

In November 2018, a consulting firm engaged by the FDIC to assess the effectiveness of the internal network security controls identified [redacted]

**Protection of Sensitive Information (Protect – Data Protection and Privacy).** Federal law, NIST security standards and guidelines, and OMB policy require agencies to safeguard sensitive information stored in electronic and hard copy format from unauthorized access or disclosure. The FDIC did not adequately restrict access to sensitive information stored on its internal network or in its building facilities based on business needs. Such information included sensitive PII, such as employee names, addresses, and Social Security Numbers; confidential bank examination information; financial investigation case files; procurement sensitive information; attorney-client privileged information; suspicious activity reports; and employee administrative actions. In many cases, sensitive hardcopy information was stored in unlocked filing cabinets, boxes in hallways, and other common building areas. The lack of proper access control over this information increased the risk of insider threats and the potential for breaches. Such incidents expose the FDIC to potential unnecessary costs and legal liability.

**Security and Privacy Awareness Training (Protect – Security Training).** FISMA requires agencies to provide security awareness training to their personnel, including contractors. FDIC policy also requires employees and contractor personnel with network access to complete security and privacy awareness training within one week of employment, and annually thereafter. Access to network applications and systems is revoked for individuals who fail to comply with this requirement. We identified 29 network users who did not complete the FDIC's security and privacy awareness training, yet who maintained their access to the network. The FDIC was not aware of the 29 users because the system used to monitor training compliance did not track all users required to take the annual security and privacy awareness training.

Users who do not complete required security and privacy awareness training are less likely to be familiar with policies, procedures, and requirements for protecting sensitive information systems and data. This increases the risk that these individuals will not comply with Federal security and privacy laws and policies, or properly protect FDIC information systems and data. It is, therefore, important that network users complete required security and privacy awareness training to ensure they understand their responsibilities for safeguarding the FDIC's network, systems, and data.

**Security Control Assessments (Detect – ISCM).** FISMA requires agencies to test and evaluate their information security controls periodically to ensure that they are effectively implemented. The FDIC regularly assesses security control requirements following a risk-based schedule, as recommended by

NIST. However, in its report entitled *Security Configuration Management of the Windows Server Operating System,* dated January 2019,[15] the FDIC OIG identified instances that occurred in 2016 and 2017 in which security control assessors did not test the implementation of security controls, when warranted. Instead, assessors relied on narrative descriptions of controls in FDIC policies, procedures, and system security plans and/or interviews of FDIC or contractor personnel. Without testing, assessors lacked a basis for concluding on the effectiveness of security controls. The FDIC relies on the results of these security control assessments to support a number of key risk management activities. These activities include identifying security weaknesses in the FDIC's information systems and IT environment; prioritizing risk mitigation activities; confirming the resolution of known security weaknesses; informing security authorization decisions; and supporting resource allocation decisions.

The FDIC OIG made three recommendations related to the FDIC's security controls assessment process and oversight. In August 2019, the FDIC provided its corrective action closure packages for the recommendations. At the close of the audit, the FDIC OIG had not yet completed its review of the corrective action packages.

# AUDIT RESULTS

## IDENTIFY

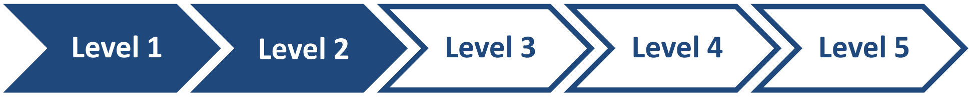
The objective of the *Identify* function is to develop an organizational understanding of how to manage cybersecurity risks to agency systems, assets, data, and capabilities. The NIST Cybersecurity Framework highlights risk management processes that organizations can implement to inform and prioritize decisions.

### Risk Management

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 (an acceptable level of variance in performance relative to the achievement of objectives). 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. Further, implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cybersecurity programs. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.

[15] OIG Report, *Security Configuration Management of the Windows Server Operating System* (FDIC OIG AUD-19-004) (January 2019).

**Figure 3: Maturity Rating - Risk Management**



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

In July 2016, OMB issued an updated Circular Number A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (OMB Circular A-123), to ensure Federal officials effectively manage risks that could affect the achievement of agency strategic objectives.[16] OMB Circular A-123 requires agencies to implement an ERM capability. According to the Circular, ERM is an effective agency-wide approach to addressing the full spectrum of the organization's external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos. ERM provides an enterprise-wide, strategically-aligned portfolio view of organizational challenges, which provides better insight about how to most effectively prioritize resource allocations to ensure successful mission delivery.

OMB Circular A-123 encourages Federal agencies to establish a risk management governance structure that includes a Risk Management Council;[17] a Risk Appetite;[18] Risk Tolerance levels; and Risk Profiles,[19] including plans for developing the depth and quality of those risk profiles over time. According to OMB Circular A-123, agencies should consider risks as part of their annual strategic review processes. The FDIC took steps following our FISMA audit in 2018 towards aligning its risk management activities with OMB policy and NIST guidance. Specifically, the FDIC:

- Revised FDIC Directive 4010.3, *Enterprise Risk Management and Internal Control Program*, in October 2018 in response to the re-issuance of OMB Circular A-123. FDIC Directive 4010.3 outlines the components of the FDIC's ERM program, including its governance structure and key roles and responsibilities;
- Approved a charter for the IT Risk Advisory Committee (ITRAC) [20] in January 2019 (subsequently updated in April 2019). Members of ITRAC collaborated with the Division of Finance's Risk Management and Internal Controls (RMIC) Branch to improve the FDIC's IT risk management capabilities;

[16] 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.

[17] OMB Circular A-123 states that to provide governance 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.

[18] OMB Circular A-123 states that senior agency leadership should establish the risk appetite, which serves as a guidepost to establish strategy and select objectives and a risk tolerance.

[19] OMB Circular A-123 states that "the primary purpose of the Risk Profile is to provide a thoughtful analysis of the risks an agency faces toward achieving its strategic objectives arising from its activities and operations, and to identify appropriate options for addressing significant risks. The risk profile differs from a risk register in that it is a prioritized inventory of the most significant risks identified and assessed through the risk assessment process versus a complete inventory of risks."

[20] The ITRAC replaced the former Information Security Risk Advisory Council in July 2018.

- Issued a Risk Appetite statement in April 2019 outlining the FDIC's position on risk, as well as the level of risk that is acceptable in pursuing the FDIC's strategic goals and objectives;
- Created a dedicated ERM Unit within RMIC in May 2019 to work across Division and Office lines to identify, assess, mitigate, and monitor the full spectrum of risks facing the FDIC; and
- Issued the FDIC's Enterprise Risk Management Standard Operating Procedure in May 2019 to define the activities that support the ERM program as defined in FDIC Directive 4010.3.

In addition, at the close of our audit field work, the FDIC was working to:

- Complete and Manage its Risk Inventory: RMIC developed an initial draft Risk Inventory of over 100 items and provided this to FDIC Divisions and Offices for comment in May 2019. As of September 2019, RMIC was continuing to work with FDIC Divisions and Offices to gain a better understanding of enterprise risks and opportunities, and ensure that appropriate mitigation strategies are in place. RMIC was also working to populate a newly-developed ERM tool with Risk Inventory items. When fully populated, the tool is intended to provide centralized management, tracking, and reporting of risks across the FDIC. RMIC had a goal to complete the Risk Inventory and populate the ERM tool by September 2019.
- Complete the Risk Profile: RMIC identified and prioritized significant risks facing the FDIC. However, for each risk in the Risk Profile, RMIC had not yet determined the extent to which mitigating controls existed,[21] the amount of residual risk that remained, or the direction in which risks were trending. RMIC had a goal to complete this work by December 2019.
- Address two recommendations contained in our FISMA audit report issued in 2017:[22]
    1. Develop a method and strategy for FDIC Divisions and Offices to use in classifying risk ratings and risk profiles for corporate applications and systems; and
    2. Develop and communicate the FDIC's information security Risk Tolerance level and Risk Profile used to prioritize risk mitigation activities.

The FDIC expects to complete corrective actions for both recommendations by January 2020.

Completing the Risk Inventory and Risk Profile will help ensure that the FDIC identifies and assesses all relevant risks; determines whether existing controls adequately mitigate those risks; and effectively prioritizes resources towards addressing those risks. In April 2019, the FDIC OIG initiated a separate evaluation to assess the effectiveness of the FDIC's ERM program implementation efforts. The FDIC OIG will make recommendations, as appropriate, as part of the ERM evaluation.

We are not making any additional recommendations in this area.

[21] OMB Memorandum 18-16, *Appendix A to OMB Circular No. A-123, Management of Reporting and Data Integrity Risk* (June 2018), states "A critical component of developing the risk profile is the determination by management of those risks in which the application of formal internal control activities is the appropriate risk response."

[22] These two recommendations are listed in Appendix I as Recommendations 4 and 5 from the FISMA audit report issued in 2017.

**IT Modernization and Cybersecurity Workforce**

We identified a key risk facing the FDIC that is linked to the modernization of the FDIC's IT environment and cybersecurity workforce. In December 2018, the FDIC's Board of Directors approved $1.5 million for the development of an IT Modernization Plan. The CIOO completed this plan in July 2019 and immediately began using it to support IT-decision making. The IT Modernization Plan lays out an approach for remediating obsolete technologies in the FDIC's IT environment that are becoming increasingly fragile, unreliable, and costly to maintain. Modernizing the IT environment will introduce significant changes in how the CIOO develops and delivers IT services and products. For example, the Modernization Plan emphasizes the adoption of common and shared IT solutions, such as cloud computing, that meet the broad needs of the FDIC. In contrast, the FDIC has historically designed custom IT solutions to meet the needs of individual business functions or units. According to the IT Modernization Plan, changes in the delivery of IT services will require the CIOO to consider corresponding changes in the competencies, skills, and abilities needed for its IT workforce, including its cybersecurity professionals.

As of August 21, 2019, the CIOO employed 327 full-time employees and 1,005 contractor personnel. Of the 1,005 contractor personnel, [redacted] were assigned to the ISC-3 Contract.[23] The ISC-3 Contract supports the day-to-day operations of FDIC's IT infrastructure facilities, hardware, software, and systems. This includes operational security, client support/help desk functions, data center operations, asset management, and systems engineering. Therefore, the ISC-3 contractor is critical to the successful implementation of the IT Modernization Plan.

The ISC-3 Contract is approaching the end of its term. As a result, the FDIC issued a Request for Proposals on July 22, 2019, for a potential $487.5 million basic ordering agreement to replace the ISC-3 Contract. Re-competing large and complex contracts like the ISC-3 Contract presents certain risks, such as the potential for competing contractors to file bid protests related to the solicitation or award of the contract. Such a protest would require the FDIC to expend resources to defend its procurement decisions, potentially delaying the acquisition of IT services and resulting in the loss of institutional knowledge should incumbent contractor personnel leave the FDIC to find other employment. The FDIC experienced such risks beginning in 2012, when the former incumbent contractor for infrastructure services pursued bid protests that delayed the award of the contract.

Both OMB and the Federal IG community have identified the planning and acquisition for modernizing IT infrastructure and the recruitment and retention of a highly skilled cybersecurity workforce as a top challenge facing the Federal Government. In addition, OMB Circular Number A-130, *Managing Information as a Strategic Resource* (OMB Circular A-130), dated July 2016, states that agencies must develop and maintain a current workforce planning process to ensure that the agency can maintain workforce skills in a rapidly developing IT environment and recruit and retain the IT talent needed to accomplish the agency's mission. As the FDIC implements its IT Modernization Plan and concurrently re-competes its ISC-3 Contract, it must ensure adequate consideration is given to information security and its cybersecurity workforce planning. In this regard, the FDIC OIG made a recommendation in its

[23] The ISC-3 Contract is a Government–Wide Acquisition Contract administered through and managed by the General Services Administration's Federal Systems Integration and Management Center, which provides acquisition services to Federal agencies.

report, entitled *The FDIC's Governance of Information Technology Initiatives*, dated July 2018,[24] to identify and document the IT resources and expertise needed to execute the FDIC's IT Strategic Plan. In response, the CIOO has undertaken a workforce planning analysis to examine the readiness of the current IT workforce against future requirements, identify gaps, and implement strategies to close gaps. This analysis is considering the needs associated with the IT Modernization Plan. The success of the workforce planning analysis is critical for ensuring that the FDIC's information systems and data remain reliable, secure, and capable of supporting mission-essential functions.

### Prior Year Recommendations

The FDIC was working to address three recommendations made in prior year FISMA audit reports that are linked to Risk Management.

> **Contractor Assessments.** In our FISMA audit report issued in 2015, we noted that the FDIC had not performed timely assessments of its contractor ("outsourced") information service providers as required by the FDIC's Outsourced Information Service Provider Assessment Methodology. 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 timely completion of the assessments.[25] In response, the CIOO published an updated FDIC Outsourced Solution Assessment Methodology in November 2018 and improved the tracking and reporting of risks associated with outsourced vendors. The FDIC provided the OIG with corrective action closure documentation for the prior year recommendation after the close of our audit field work. The OIG is reviewing this documentation as part of its audit follow-up process. The prior year recommendation will remain open until the OIG determines that the corrective action closure documentation is responsive.
>
> **DCOM Security Weaknesses.** In our FISMA audit report issued in 2016, we noted that the FDIC had not addressed a number of security weaknesses in DCOM with a threat level of moderate. CIOO officials informed us that due to limited resources, they had focused their resources on higher priority projects and efforts to address weaknesses with a threat level of high. We made a recommendation in our FISMA audit report issued in 2016 that the CIO review existing resource commitments and priorities for addressing DCOM POA&Ms and take appropriate steps to ensure they were addressed in a timely manner.[26] In response, the CIOO updated its POA&M policy and procedures in March 2019 and May 2019, respectively, to provide guidance on (among other things) establishing remediation timeframes based on risk scores to assist in resource allocations. The CIOO also reviewed its existing resource commitments and priorities for addressing DCOM POA&Ms. At the end of our field work, RMIC was reviewing the corrective actions for this recommendation and working with the CIOO to ensure it adequately addressed agreed-upon actions.[27] Therefore, our prior recommendation remains open.

[24] OIG Report, *The FDIC's Governance of Information Technology Initiatives* (FDIC OIG AUD 18-004) (July 2018).
[25] This recommendation is listed in Appendix I as Recommendation 4 from the FISMA audit report issued in 2015.
[26] This recommendation is listed in Appendix I as Recommendation 5 from the FISMA audit report issued in 2016.
[27] RMIC has responsibility for reviewing corrective actions taken by FDIC Divisions and Offices in response to GAO and OIG recommendations. When RMIC determines that corrective actions are responsive, RMIC provides GAO or the OIG with documentation supporting that corrective actions have been taken by the FDIC.

**Evaluating Security Risks.** In our FISMA audit report issued in 2017, we determined that the FDIC assigned risk ratings of high, moderate, or low for weaknesses in POA&Ms and risk ratings of high, critical, moderate, low, or informational for vulnerabilities identified through its scanning processes. However, the FDIC had not evaluated the collective risk associated with security weaknesses and vulnerabilities. We recommended in our FISMA audit report issued in 2017, that the CIO develop an approach and implement procedures for evaluating the collective risk associated with known security weaknesses and vulnerabilities to ensure they collectively remained within established risk tolerance levels.[28] In response, the CIOO developed procedures in May 2019 intended to ensure that known security weaknesses and vulnerabilities are fully integrated into the CIOO's risk management processes. At the end of our field work, RMIC was reviewing the corrective actions for this recommendation and working with the CIOO to ensure it adequately addressed agreed-upon actions. Therefore, our prior recommendation remains open.

## PROTECT

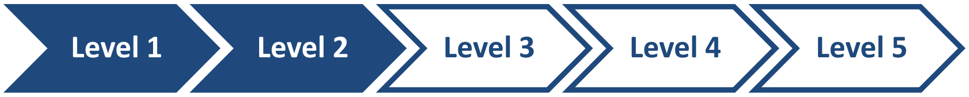
The objective of the *Protect* function is to develop and implement safeguards to secure information systems. The *Protect* function supports the ability to prevent, limit, or contain the impact of a cybersecurity event through configuration management, identity and access management, data protection 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 controlling the processes for initializing, changing, and monitoring their configuration throughout the system development life cycle.

FISMA requires 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**



[28] This recommendation is listed in Appendix I as Recommendation 15 from the FISMA audit report issued in 2017.

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

The FDIC has defined and implemented key Configuration Management processes and controls recommended by NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, dated August 2011. For example, the FDIC documented baseline configurations[29] for its core IT infrastructure, including the Windows Servers and DCOM systems; used an automated change management system to track, manage, and report information about proposed and approved configuration changes; and governed changes through a formal Change Control Board. However, as described below, the FDIC was working to strengthen controls with respect to: (i) monitoring and compliance reporting for baseline configurations; (ii) management of security patches; (iii) practices for conducting credentialed scans; and (iv) management of network firewall rules.

***Monitoring and Compliance Reporting for Baseline Configurations***

The FDIC monitors compliance with its baseline configurations through a combination of automated scanning and manual assessments. Such activities help to ensure that the FDIC's information systems are properly secured to mitigate against cyberattacks. CIOO Policy 16-005, *Policy on Secure Baseline Configuration Guides,* dated December 2016, states that the OCISO has responsibility for scanning information systems to determine whether they comply with applicable baseline configuration requirements. According to CIOO Policy 16-005, all FDIC IT products, applications, and operating systems must be at least 95-percent compliant with their associated baseline configuration.[30] CIOO Policy 16-005 also requires the OCISO to perform manual reviews of configuration settings that cannot be monitored through scans or other automated tools.

In our FISMA audit report issued in 2018, we noted that CIOO Policy 16-005 did not describe how the results of OCISO's manual reviews factored into the CIOO's determination of whether a system is 95-percent compliant with its associated baseline configuration. We recommended in our previous FISMA audit report that the CIO develop and implement procedures that define how the results of manual configuration reviews are considered when determining whether IT products, applications, and operating systems are 95-percent compliant with their approved baseline configurations.[31] In response, the CIOO developed a new *Secure Baseline Configuration Guide (SBCG) Process and Procedures* document. At the end of our field work, RMIC was reviewing the corrective actions for this recommendation and working with the CIOO to ensure it adequately addressed agreed-upon actions. Therefore, our prior recommendation remains open.

We are not making any additional recommendations in this area.

[29] A baseline configuration is a document or repository containing a set of specifications for an information system that can only be changed through a formal change control process. Agencies 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.

[30] FDIC CIOO Policy 16-005 states that the compliance score should be calculated as the total number of security controls in the approved baseline that were compliant divided by the total number of security controls assessed for a given baseline.

[31] This recommendation is listed in Appendix I as Recommendation 2 from the FISMA audit report issued in 2018.

### *Patch Management*

NIST SP 800-40, Revision 3, *Guide to Enterprise Patch Management Technologies*, dated July 2013, defines patch management as the process of identifying, acquiring, installing, and verifying patches for products and systems. Software vendors release patches on a periodic or as-needed basis to address faults in operating systems or applications; alter functionality or address new security threats; or modify software configurations to make systems and applications less susceptible to cyberattacks and more secure. Therefore, effective patch management is critical to mitigating the risk of system outages and malicious activity that could impair the FDIC's ability to conduct its business functions.

In our FISMA audit report issued in 2017, we noted instances in which the CIOO did not install patches addressing "high" severity vulnerabilities on servers, desktop computers, and laptop computers within established timeframes. We recommended in our FISMA report issued in 2017 that the CIO ensure that the FDIC patches its systems in accordance with its patch management policy and NIST-recommended practices.[32]

In our FISMA audit report issued in 2018, we determined that the CIOO did not fully address the prior year recommendation. Further, based on our audit work conducted in 2018, we found that the CIOO did not always create POA&Ms to capture vulnerabilities associated with overdue patches.[33] As a result, we made a recommendation in our FISMA audit report issued in 2018 that the CIO develop and implement a process to ensure that vulnerabilities resulting from patches not installed within required timeframes be tracked and reported to senior management.[34]

In response to these recommendations in 2017 and 2018, the CIOO updated its patch management policy[35] to define a new process for documenting deferrals and acceptances of risk and for creating POA&Ms when patches are not implemented within established timeframes. The CIOO also created new procedures[36] that included patch management standards, tolerances, and performance measures. Further, the CIOO established training requirements for managers on the use of the CIOO's vulnerability dashboard, which monitors compliance with patch policy requirements. CIOO representatives informed us that the CIOO began implementing the policy and procedures at the end of June 2019. The FDIC provided the OIG with corrective action closure documentation for both prior year recommendations after the close of our audit field work. The OIG is reviewing this documentation as part of its audit follow-up process. Both prior year recommendations will remain open until the OIG determines that the corrective action closure documentation is responsive.

We are not making any additional recommendations in this area.

[32] This recommendation is listed in Appendix I as Recommendation 9 from the FISMA audit report issued in 2017.
[33] A memorandum issued by the OCISO on November 1, 2017, mandated that a POA&M be created whenever a patch is not implemented within required timeframes.
[34] This recommendation is listed in Appendix I as Recommendation 4 from the FISMA audit report issued in 2018.
[35] FDIC CIOO Policy 19-005, *Policy on Security Patch Management* (April 2019).
[36] FDIC, *CIOO Patch Management Standard Operating Procedure Version 2.4* (June 2019) and FDIC,*Vulnerability Compliance Reporting Version 1.0* (June 2019).

### *Credentialed Scans*

NIST SP 800-123, *Guide to General Server Security*, dated July 2008, states that organizations should conduct vulnerability scanning to validate that operating systems and server software are current with regard to security patches and software versions. NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated April 2013, recommends that organizations use privileged access when conducting vulnerability scans of IT systems and devices. Privileged access allows the scanning tool to log into the device being scanned, to enable it to thoroughly inspect the device for vulnerabilities. Such scans are sometimes referred to as credentialed scans. Credentialed scans are a key control for ensuring that the FDIC has complete and accurate information about the security posture of the IT assets connected to the network. As such, any limitations on their effectiveness should be promptly addressed.

In our FISMA audit report issued in 2017, we identified 132 network IT devices for which the CIOO's scanning tool did not perform a successful credentialed scan for a period of more than 30 days. In many cases, a successful credentialed scan did not occur because the scanning tool did not have the appropriate administrative access to log into the IT device to perform a credentialed scan. As a result, we reported that the 132 IT devices may have unidentified vulnerabilities that presented security risks to the FDIC's IT environment. We recommended in our FISMA audit report issued in 2017 that the CIO review and enhance the FDIC's vulnerability scanning processes to ensure that issues associated with conducting credentialed scans are resolved in a timely manner.[37]

In our FISMA audit report issued in 2018, we noted that the OCISO had developed the *Patch & Vulnerability Group (PVG) Authentication Failures Ticket Overview* document to address instances in which the scanning tool did not have the appropriate administrative access to log into the IT device to perform a credentialed scan. The procedures within this document required DIT staff to create Help Desk tickets[38] to track the resolution of such instances. As part of our FISMA audit conducted in 2018, we determined that although DIT created Help Desk tickets on a weekly basis that identified IT assets not subject to a successful credentialed scan, DIT often closed the tickets before all of the IT assets listed on them had been resolved and opened new tickets with the same IT assets on them. This practice resulted in some IT assets not being resolved timely and limited the CIOO's ability to investigate and remediate the root causes of why IT assets were not subject to a successful credentialed scan.

Following our FISMA audit in 2018, the CIOO took several actions to address our recommendation made in 2017. Specifically, the CIOO began tracking credentialed scanning authentication failures via a dashboard, and the Vulnerability Management Team began briefing executive management on credentialed scanning compliance. Further, the CIOO issued the *Scan Authentication and Failure Remediation Standard Operating Procedures*, dated May 2019, to guide the identification, reporting, and remediation of credentialed scanning errors. At the end of our field work, RMIC was reviewing the corrective actions for this recommendation and working with the CIOO to ensure it adequately addressed agreed-upon actions. Therefore, our prior year recommendation remains open.

[37] This recommendation is listed in Appendix I as Recommendation 10 from the FISMA audit report issued in 2017.

[38] The DIT Help Desk is an IT support service available to FDIC employees and contractors who need help with IT-related issues and problems. The DIT Help Desk opens tickets in ServiceNow—the FDIC's automated change management system of record—to track, manage, and report IT issues.

We are not making any additional recommendations in this area.

### *Network Firewall Management*

According to NIST,[39] firewalls are essential devices or programs that help organizations protect their networks and information systems from hostile attacks, break-ins, and malicious software. The FDIC deploys firewalls at both the perimeter and interior of its network. The perimeter firewalls control the flow of inbound and outbound traffic between the Internet and the internal network. The perimeter firewalls control inbound traffic through the use of "ingress" rules that inspect traffic and permit or deny requests for access to FDIC systems. Ingress rules help to prevent external cyber threats, such as malicious software known as malware, from entering the network. The perimeter firewalls also use "egress" rules to control outbound traffic. By controlling the type of traffic allowed to flow out of the network, the FDIC can prevent unwanted communication should a network IT device, such as a server, become compromised by an attacker or malware. This reduces the risk of unauthorized exfiltration of sensitive FDIC information. Therefore, the FDIC's firewalls are only as effective as the rules that the FDIC defines for them.

In its audit report, entitled *Preventing and Detecting Cyber Threats,* dated May 2019, the FDIC OIG reported a number of weaknesses that limited the effectiveness of the FDIC's network perimeter and interior firewalls.[40] According to the OIG's report, many firewall rules lacked a documented justification, and the majority of rules were unnecessary. Several factors contributed to these weaknesses, including an inadequate firewall policy and supporting procedures, and an ineffective process for periodically reviewing firewall rules to ensure their continued need. Unnecessary firewall rules pose a security risk [redacted] The FDIC took significant steps during our audit to address the weaknesses identified in the FDIC OIG's report. However, the FDIC had not yet completed actions to document all existing network firewall rules with an approval and mission/business need, including the duration of that need, and implement a firewall policy consistent with NIST guidance. The FDIC plans to complete these actions by January 2020.

We are not making any additional recommendations in this area.

### *Web-Application Vulnerabilities*

The FDIC engaged a consulting firm to conduct a penetration test of the FDIC's external network. The consulting firm performed the penetration test from November 2018 through December 2018 from the perspective of an Internet-connected attacker. The consulting firm's report, which was issued in January 2019, contained 10 findings.[41] [redacted]

[39] NIST Information Technology Laboratory Bulletin, *Protecting Information Systems with Firewalls: Revised Guidelines on Firewall Technologies and Policies* (October 2009).

[40] FDIC OIG AUD-19-005.

[41] The FDIC created 10 POA&Ms to address the 10 findings. As of July 2019, the FDIC had closed 8 of the 10 POA&Ms.

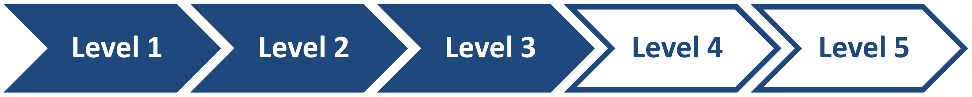
[redacted][42][redacted]

We are not making any additional recommendations in this area.

### 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 that their access is limited to the minimum necessary to perform their jobs. This includes performing personnel screening and onboarding, issuing and maintaining user credentials (usernames and passwords), and managing logical and physical access privileges, which are collectively referred to as ICAM.

**Figure 5: Maturity Rating - Identity and Access Management**



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

In 2017, the FDIC began requiring all eligible employees and contractor personnel to use their personal identity verification (PIV) card[43] to authenticate to the network via desktop and laptop computers. In July 2017, the FDIC issued Circular 1600.8, *Personal Identity Verification Card Program*. FDIC Circular 1600.8 defines the FDIC's policy and responsibilities regarding the use of PIV cards for gaining physical access to FDIC owned/leased space and logical access to FDIC information systems. In May 2019, OMB issued Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*. The OMB Memorandum established a roadmap for modernizing ICAM implementations within the Federal Executive branch. In response, the FDIC issued an *ICAM Strategy*, established an *ICAM Program Charter*, and developed an *ICAM Segment Architecture*.[44] Collectively, these documents are intended to guide the FDIC's ICAM activities, address Federal ICAM (FICAM)

[42] [redacted]

[43] A PIV card is a hand-carried identity credential issued by a Federal Government entity. A PIV card contains a computer chip with data that allows the cardholder to be granted access to Federally-controlled facilities and information systems.

[44] The FDIC issued the *ICAM Strategy* document, *ICAM Program Charter*, and *ICAM Segment Architecture*, in July 2019. The *ICAM Strategy* is intended to lay a foundation for a comprehensive and integrated approach to ICAM at the FDIC. The *ICAM Strategy* identifies key initiatives that will implement the ICAM Strategy. The *ICAM Program Charter* establishes the structure and governance over the ICAM Program, including its goals. The *ICAM Segment Architecture* provides the technical framework, goals, and objectives for the ICAM program.

requirements, and help ensure alignment with the FICAM Architecture.[45]

### *Privileged Account Management*

The FDIC assigns "administrative accounts" to certain network users. These administrative accounts have privileged (elevated) access to systems and network IT resources to perform maintenance and other types of necessary IT troubleshooting activities. Administrative accounts can create new accounts, change configuration settings, and bypass system controls. For these reasons, hackers and other adversaries target administrative accounts to perform malicious activity. A compromise of an administrative account would pose significant risks to the FDIC's IT environment. For example, an administrative account could be used by a malicious actor to exfiltrate sensitive information from the internal network or to disrupt critical IT services. As a result, administrative accounts must be carefully controlled and monitored.

In its report, entitled *Preventing and Detecting Cyber Threats*, dated May 2019,[46] the FDIC OIG identified instances in which administrative accounts on the [redacted] network firewalls did not always require users to uniquely identify and authenticate when accessing the firewalls.[47] NIST SP 800-53, Revision 4, recommends that Federal information systems uniquely identify and authenticate individuals who access these systems. Doing so allows agencies to monitor an individual's activity within the system and perform after-the-fact investigations if malicious activity occurs. The FDIC OIG's report also noted instances in which [redacted] This vulnerability exposed the network firewalls to increased risk of unauthorized access or malicious activity. We noted a similar vulnerability during our FISMA audit conducted in 2017, [redacted]. The CIOO took steps to address the administrative account management issues described in the FDIC OIG's report on *Preventing and Detecting Cyber Threats* in 2018 and 2019.

In November 2018, the FDIC engaged an external consulting firm to assess the effectiveness of its internal network security controls. As part of its assessment work, the consultant tested network security controls using techniques commonly associated with malicious threat actors. The consultant's report, which was issued in January 2019, contained 11 findings, [redacted]

- [redacted]
- [redacted]

[45] The FICAM Architecture is the Federal Government's approach for designing, planning for, and implementing ICAM. It depicts principles and practices in the form of diagrams and stories to describe what ICAM is, what it should do, and what it is used for, in order to provide capabilities to an agency.
[46] FDIC OIG AUD-19-005.
[47] Identification is the process of uniquely identifying a user or process that accesses an information system. Authentication is the process of verifying the user or process is genuinely who or what they claim to be. For example, an information system may uniquely identify a user though his/her User ID and authenticate the user by checking that the supplied password is correct.

- [redacted]

[redacted]

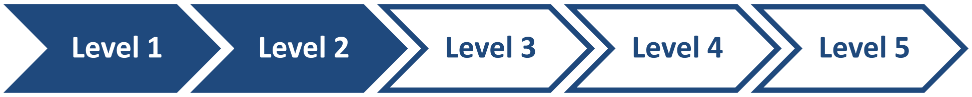
[redacted]

We are not making any additional recommendations in this area.

### Data Protection and Privacy

*Data Protection and Privacy* includes determining the extent to which the organization has developed a privacy program to protect PII that is collected, used, maintained, shared, and disposed of by information systems. An organization must consider the data lifecycle[48] and associated security controls to protect PII, encryption of data at rest and in transit, controls over removable media, data exfiltration controls, and privacy breach response plans.

**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.[49] OMB Circular A-130 requires agencies to:

- Reduce their PII holdings to the minimum amount necessary for the proper performance of authorized agency functions;
- Conduct privacy impact assessments, as prescribed by the E-Government Act of 2002,[50] when

[48] According to the FDIC Enterprise Architecture Blueprint, the data lifecycle refers to the manner in which all FDIC data (structured and unstructured) are managed and stored from the initial acquisition of the data until it is archived to offline storage.
[49] 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 2016).
[50] Section 208 of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (codified at 44 U.S.C. § 3501 note) requires agencies to conduct Privacy Impact Assessments of IT and collections of information and make them available to the public. A Privacy Impact Assessment is a process for examining the risks of using IT to collect, maintain, and disseminate PII from or about members of the public.

the agency develops, procures, or uses IT to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII;

- Implement the Risk Management Framework (RMF)[51] in NIST SP 800-37, *Guide to Applying the Risk Management Framework to Federal Information Systems and Organizations*,[52] when categorizing information systems;[53] selecting, implementing, and assessing controls; authorizing systems to operate;[54] and monitoring controls; and
- Establish and maintain an agency-wide Privacy Continuous Monitoring (PCM) strategy and PCM program.[55]

FDIC Circular 1360.20, *Privacy Program*, dated March 2013, states that it is the policy of the FDIC to protect the privacy of individuals and to collect, maintain, use, disseminate, and/or dispose of PII in accordance with applicable Federal law and OMB guidance. In fulfilling its legislative mandate, the FDIC collects and maintains significant quantities of PII on bankers, financial institution customers, depositors, and employees. In addition, as an employer and acquirer of services, the FDIC maintains significant amounts of PII related to its employees and contractors. PII maintained by the FDIC includes, but is not limited to, names, home addresses, Social Security Numbers, dates and places of birth, personal financial information, employment histories, education and healthcare information, and the results of background investigations.

FDIC Circular 1360.20 also defines the privacy-related responsibilities for individuals and component offices within the FDIC, including the CPO, Privacy Staff, Division and Office ISMs, Record Liaisons, the Legal Division, and Contracting Officers. The FDIC's CPO has overall responsibility for delivering a risk-based privacy program to help protect this PII. The FDIC's Privacy Section, a component of the OCISO, implements and manages privacy and data protection policies and procedures on behalf of the CPO. The Privacy Program focuses on ensuring that officials take appropriate steps to identify, manage, protect, and reduce the risks to PII.

In addition, the FDIC's Privacy Program Plan, issued on October 24, 2017, and updated in February 2019, provides an overview of the FDIC's Privacy Program, including its structure, resources, roles, responsibilities, strategic goals, and objectives for achieving its mission and vision of minimizing privacy risks and fostering a strong culture of privacy protection throughout the agency. This plan establishes a

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

[52] According to OMB Circular A-130, the RMF was traditionally used to help agencies address information security and related risks in the authorization process for Federal information systems. OMB Circular A-130 explains how agencies should integrate their privacy programs into the RMF process. However, many of the NIST standards and guidelines that existed when OMB Circular A-130 was published in July 2016 did not fully address the role of privacy and agencies' privacy programs. In December 2018, NIST revised SP 800-37 to (among other things) integrate privacy into the RMF.

[53] NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* (December 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.

[54] 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 an information system, 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.

[55] 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.

risk-based framework and identifies the program management and common controls for managing privacy risks and complying with applicable privacy requirements.

The FDIC OIG is conducting an audit of the FDIC's Privacy Program, the objective of which is to assess the effectiveness of the FDIC's privacy program and practices. The FDIC OIG's audit found that the FDIC implemented various controls and practices consistent with Federal privacy-related requirements and responsibilities described in OMB Circular A-130, Appendix II. Of particular note, the FDIC designated a Senior Agency Official for Privacy (SAOP);[56] implemented a privacy awareness and training program; and identified its privacy staffing and budgetary needs. The FDIC also established privacy competency requirements for key staff and took steps to ensure contractor compliance with privacy requirements. However, the FDIC's privacy controls and practices did not comply with all relevant privacy laws[57] 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 CPO or implement Records and Information Management Unit (RIMU) responsibilities for supporting the Privacy Program;[58]
- Effectively manage or secure PII stored outside of information systems or dispose of PII in accordance with the FDIC's Records Retention Schedule;[59] or
- Ensure that Privacy Impact Assessments were always completed, monitored, published, and retired in a timely manner.

During our audit, the FDIC was taking action to better align its Privacy Program with relevant privacy laws and OMB policy and guidance. For example, Privacy Section staff stated that they had modified the procedures used to perform a Privacy Threshold Analysis[60] to better address privacy considerations in the categorization of information systems. In addition, Privacy Section staff stated that they were revising the FDIC's Privacy Impact Assessments to serve as privacy plans[61] for the FDIC's information systems. The FDIC OIG plans to report the results of its Privacy Program audit and make recommendations, as appropriate, in a separate report.

[56] At the FDIC, the SAOP has the same responsibilities as the CPO.

[57] Such laws include the 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); and 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).

[58] 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. 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.

[59] 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.

[60] The FDIC conducts a Privacy Threshold Analysis whenever new information systems are developed or acquired. A Privacy Threshold Analysis determines whether systems involve the collection and use of PII, and whether a Privacy Impact Assessment and/or System of Records Notice is required. A System of Records Notice is an official public notice of an organization's system(s) of records, as required by the Privacy Act of 1974, that identifies: (i) the purpose for the system of records; (ii) the individuals covered by information in the system of records; (iii) the categories of records maintained about individuals; and (iv) the ways in which the information is shared.

[61] According to NIST SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations* (December 2014), a privacy plan is a written document that provides an overview of the privacy requirements for an information system or program and describes the privacy controls in place or planned for meeting those requirements.

We are not making any additional recommendations in this area.

### *Controls over Sensitive Information Stored in FDIC Facilities*

Federal statutes, such as the Privacy Act of 1974 and FISMA; 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.[62] In addition, FDIC Circular 1360.9, *Protecting Sensitive Information*, dated 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. FDIC Circular 1360.9 requires hardcopy sensitive information to be stored in corporate facilities, such as locked drawers, file cabinets, and file rooms whenever possible. Further, the FDIC's security and privacy awareness training program instructs employees and contractor personnel to protect sensitive data in both electronic and hardcopy formats from unauthorized access or disclosure.

On July 25, 2019, we conducted unannounced walkthroughs of selected areas within the FDIC's Virginia Square facility. The purpose of the walkthroughs was to identify portable storage media, such as CDs and DVDs, as well as hard-copy sensitive information, including PII that may not be properly secured.[63] During the walkthroughs, we identified significant quantities of sensitive hardcopy information easily accessible to anyone in the Virginia Square facility, including employees, visitors, and contractor personnel such as cleaning/janitorial staff and security guards. The majority of unsecured sensitive information we found was stored in unlocked filing cabinets and boxes in building hallways. Examples included:

- Confidential bank examination information, such as Reports of Examination;
- Suspicious Activity Reports (SAR);[64]
- Sensitive PII, such as reports containing names, Social Security Numbers, and dates of birth;
- Legal documents, analyses, and correspondence pertaining to investigations, litigation, claims, and settlements;
- Portable storage media, including a computer hard drive and CDs/DVDs (one of which was marked confidential); and
- Contracting and procurement sensitive information.

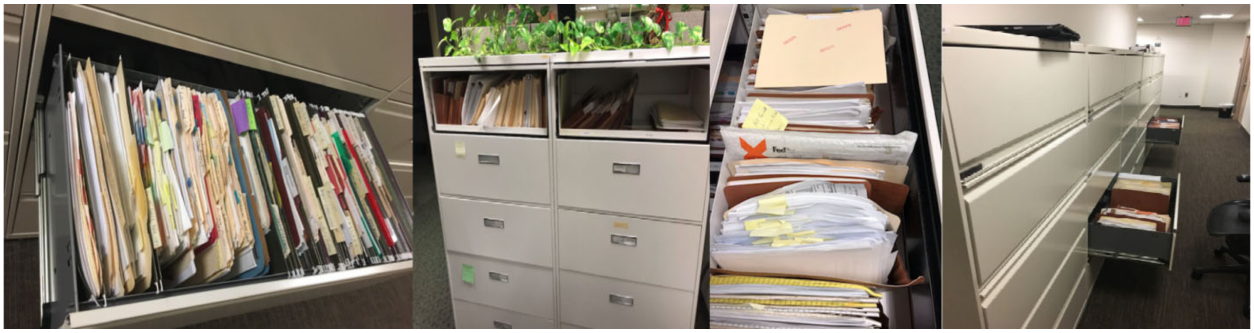
[62] The Privacy Act of 1974 states that agencies shall establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial 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, Revision 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.

[63] The walkthroughs did not include employee or contractor offices or cubicles, nor did they include restricted workspaces, such as locked rooms or areas with limited access.

[64] On November 23, 2010, the U.S. Department of the Treasury, Financial Crimes Enforcement Network, issued an advisory, entitled *Maintaining the Confidentiality of Suspicious Activity Reports*, to regulatory and law enforcement agencies, self-regulatory organizations, and financial institutions. The advisory stated that the unauthorized disclosure of SARs is a violation of Federal law and that civil and criminal penalties may be imposed for SAR disclosure violations. The advisory recommended that the referenced organizations implement robust programs to protect the confidentiality of SARs and information that would reveal the existence of a SAR.

Figure 7 illustrates examples of filing cabinets that Cotton & Company LLP and FDIC OIG employees opened during the walkthroughs to demonstrate the ease with which sensitive information could be accessed.

**Figure 7: Images of Unsecured Filing Cabinets Containing Sensitive Information**



Source: Photographs taken by FDIC OIG employees during Cotton & Company LLP's walkthroughs of the Virginia Square facility.

Although the FDIC took steps to promote awareness through policy and training among its employees and contractor personnel regarding the need to secure sensitive information, these steps were not effective. Additional emphasis on employee and contractor awareness is warranted until Divisions and Offices can ensure that sensitive information is consistently secured throughout FDIC facilities. Such emphasis could be in the form of frequent reminders by ISMs and awareness briefings during Division and Office conferences.

In addition, the FDIC did not monitor employee and contractor compliance for safeguarding sensitive information stored in FDIC facilities. Such monitoring could include performing periodic walkthroughs of FDIC facilities to determine whether employees and contractor personnel are properly securing sensitive records and files. Employees and contractor personnel are less likely to leave sensitive information unsecured if compliance controls are in place. In addition, we noted that the FDIC did not mark many of the documents containing sensitive information, including PII, to heighten awareness of the need to protect such information.

In late 2016, the FDIC initiated a multi-year initiative to identify, categorize, label, and protect the FDIC's information and data. This initiative, known as the Data Protection Program, involves:

- Establishing and implementing an agency-wide data classification scheme that includes marking and handling guidelines to better identify and safeguard sensitive information;
- Increasing awareness of data protection practices throughout the FDIC workforce to reduce the risk associated with data leakage; and
- Implementing and/or configuring automated tools, where possible, to identify and prevent potential data leakage.

When the FDIC initiated the Data Protection Program in 2016, the program focused on labeling sensitive information only. In the spring of 2019, the FDIC expanded the program to include the labeling of non-sensitive information. This delayed the implementation of the Data Protection Program as the FDIC worked to modify its data protection policy directive and associated guidance to reflect the expanded scope of the program.

At the close of our audit field work, the FDIC had drafted, but not yet finalized or issued, a data protection policy directive, labeling guide, and associated job aids. The FDIC had also engaged an outside vendor to develop an automated solution to implement the Data Protection Program. CIOO officials informed us that the CIOO plans to pilot test its new process for labeling information before the end of 2019, and to finalize a policy and guidance and begin FDIC-wide implementation in 2020. Until the FDIC implements the Data Protection Program, there is an increased risk that sensitive data will not be properly handled and safeguarded as prescribed in FDIC policy.

We notified FDIC management and the Computer Security Incident Response Team (CSIRT) of the unsecured information we identified during our walkthroughs so prompt action could be taken to secure the information. FDIC officials advised that they were taking actions to ensure that all sensitive information stored in headquarters, regional, and field office locations was properly secured. For example, the FDIC's CIO requested that Division and Office Directors review all hard copy information in the custody of their division or office and confirm that it is properly secured. FDIC officials also advised that they were working to ensure that the FDIC's policies related to the proper retention, storage, and disposition of paper records, electronic records, and portable media were being followed.

### *Controls over Sensitive Information Stored on Network Shared Drives*

FDIC policy authorizes employees and contractor personnel to store business records, including records containing sensitive information, on the FDIC's internal network shared drives. According to information provided by DIT in May 2019, the FDIC's internal network contained over 200 resource servers capable of supporting shared drives. Each of these shared drives is capable of storing a significant number of documents. For example, during the ongoing audit of the FDIC's Privacy Program, the FDIC OIG observed one network shared drive that contained over 35,000 folders.

As part of its ongoing audit of the FDIC's Privacy Program and Practices, the FDIC OIG reviewed a judgmental selection of six network shared drives and found instances in which sensitive information, including sensitive PII, was not properly secured. According to DIT officials, this sensitive information was accessible to anyone with access to the FDIC's internal network, including FDIC employees and contractor personnel. Sensitive information not properly secured included:

- Names, Social Security Numbers, home addresses, and dates of birth of FDIC employees and failed bank customers;
- Names of employees who had been subject to disciplinary actions, such as letters of reprimand, suspensions, and terminations;
- Names of employees who had been placed on performance improvement plans or subject to wage garnishments; and
- Employee performance appraisals.

On June 7, 2019, the FDIC OIG notified the CIO, CPO, and CISO of the unsecured sensitive information found on the six network shared drives.[65] In its notification, the OIG stated that while it had only selected and reviewed a sample of six drives, it was likely that there was additional sensitive information stored on the internal network that was not properly secured. Accordingly, the OIG's notification stated that the FDIC should review all shared drives for potentially unsecured sensitive information. In a written response, CIOO management officials concurred with the OIG and described short-term and long-term actions it planned to take to address the vulnerability.[66]

In the short term, the CIOO will use its data loss prevention tool to scan the internal network shared drives to identify sensitive information. Once the CIOO identifies this information, it will determine the owner of the information and work with the owners to limit access to the information to appropriate personnel. The CIOO expects to complete initial scans of the network shared drives and complete any needed remediation work by December 31, 2019. The CIOO also plans to develop a long term solution to better store FDIC sensitive information by December 31, 2019.

The lack of proper access control over sensitive electronic and hard copy information, including PII, increased the risk of insider threats[67] and the potential for a breach. Breaches can lead to identity theft or other forms of consumer fraud against individuals. They can also expose the FDIC to unnecessary costs and potential legal liability.

Recommendations

We recommend that the CIO:

1. Reinforce to employees and contractor personnel the importance of properly safeguarding sensitive electronic and hardcopy information.
2. Monitor employee and contractor compliance with policy requirements for properly safeguarding sensitive electronic and hardcopy information.

**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

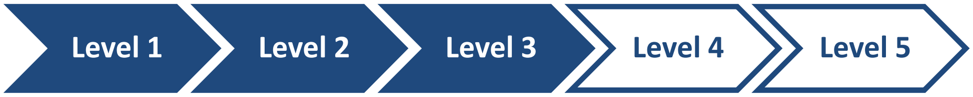
[65] FDIC OIG Advisory Memorandum, *Unsecured Sensitive Information on the Network Shared Drives* (June 2019).

[66] FDIC Memorandum, *Management Response to the Advisory Memorandum Entitled Unsecured Sensitive Information on the Network Shared Drives ~ No. 2018-018* (June 2019).

[67] According to FDIC Circular 1600.7, *FDIC Insider Threat and Counterintelligence Program* (September 2016), the term, "insider threat," refers to a threat posed to the FDIC or national security by someone who misuses or betrays, wittingly or unwittingly, his or her authorized access to a government resource. This threat may include unauthorized disclosure of unclassified sensitive information.

facilitate job performance.[68]

**Figure 8: Maturity Rating – Security Training**



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

FDIC Circulars 1360.16, *Mandatory Information Security Awareness Training*, dated March 2012, and 1360.9, *Protecting Sensitive Information*, dated April 2007, 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 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 one week of employment, and annually thereafter, will have their access to network applications and systems revoked.

The FDIC uses its learning management system, FDICLearn, to monitor compliance with the annual security and privacy awareness training requirement. FDICLearn generates a compliance report that tracks network users who comply or fail to comply with the training requirement. As of May 10, 2019, the compliance report showed that 7,198 of 7,216 (99.8 percent) network users complied with the security and privacy awareness training requirement. However, as described below, we identified additional network users who failed to comply with this requirement.

We compared the population of network users in the compliance report generated by FDICLearn as of May 10, 2019, to the population of active network user accounts in the Microsoft Windows Active Directory®[69] as of May 9, 2019. Our comparison identified 101 network user accounts in the Microsoft Windows Active Directory® that were not contained in the compliance report generated by FDICLearn. We brought this discrepancy to the attention of CIOO staff, who coordinated with the FDIC's Corporate University—the owner of FDICLearn—to determine why the discrepancy occurred. Representatives of the CIOO and Corporate University subsequently informed us that compliance reports generated by FDICLearn did not include all network users due to an error in how FDICLearn determined the employment status for certain individuals.[70] Further, of the 101 network users that we identified as missing from the compliance report, 29 had not satisfied the annual security and privacy awareness

[68] 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.

[69] The Microsoft Windows Active Directory is an IT service within the Windows Server® operating system platform that is used to centrally manage user accounts and security settings (including access).

[70] FDICLearn obtains employment status information, such as the date an individual started employment with the FDIC, from the FDIC's Corporate Human Resources Information System-Human Resources (CHRIS-HR)—the FDIC's system of record for managing personnel information. FDICLearn uses employment status information to schedule security and privacy awareness training for network users and to track their compliance.

training requirement.[71] Because these 29 users did not appear on the compliance report, the FDIC was not aware of their noncompliance and did not restrict the users' network access.

The use of reliable information to support business decision making is a basic tenet of an effective internal control system. Without reliable information in the compliance reports generated by FDICLearn, the FDIC cannot ensure that users of its network will comply with the policy requirement to complete security and privacy awareness training on an annual basis. Individuals who do not complete security and privacy awareness training are less likely to be familiar with policies, procedures, and requirements for protecting sensitive information systems and data. This increases the risk that these individuals will not comply with Federal security and privacy laws and policies, or properly protect FDIC information systems and data. Completing required security training is critical to safeguarding the FDIC's network, systems, and data, and for ensuring that individuals understand that they will be held accountable for their behavior on the network.

CIOO representatives informed us that they took steps to ensure that 27 of the 29 network users completed the security and privacy awareness training requirement. DIT restricted network access for the remaining two users. Further, a representative of Corporate University informed us that staff in Corporate University were performing a daily comparison of information in FDICLearn to CHRIS-HR to help ensure that all network users comply with the annual security and privacy awareness training requirement.

Recommendation

We recommend that the CIO:

3. Implement controls that ensure FDICLearn maintains accurate and complete information regarding user compliance with the FDIC's security and privacy awareness training requirement.

## 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.

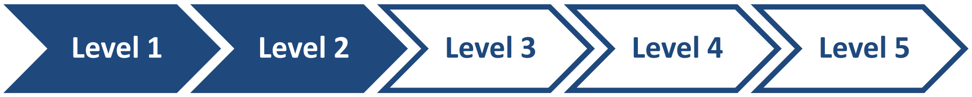
### Information Security Continuous Monitoring

OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*, dated 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*, dated September 2011, recognizes an organization-wide approach to continuous monitoring that supports

[71] CIOO representatives informed us that the remaining 72 users had either taken the required security and privacy awareness training or had their network access restricted.

risk-based decision making at the organization, mission/business process, and information systems tiers. NIST defines continuous monitoring as the process of maintaining an ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. An effective continuous monitoring program provides timely information and insights into security control effectiveness for senior leaders to make ongoing risk-based decisions affecting their mission and business functions.

**Figure 9: Maturity Rating – Information Security Continuous Monitoring**



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

The FDIC ISCM program is intended to provide FDIC management ongoing awareness of information security, vulnerabilities, and threats through various processes, controls, and tools implemented across the CIOO. Using dashboards and other reporting mechanisms, the FDIC monitors the security state of its information systems. The FDIC is in the process of procuring and implementing the Department of Justice's Cyber Security Assessment and Management (CSAM) tool to support and automate the FDIC's security assessment processes, such as its information system inventory, POA&M management, and security documentation.[72]

***Security Control Assessments***

A key component of the FDIC's ISCM is its Security Controls Assessment program. The objective of the program is to conduct ongoing risk-based evaluations of security controls to provide the FDIC with assurance that controls both within an information system, or inherited by a system, are operating effectively. NIST SP 800-53A, Revision 4, provides organizations with recommended procedures for conducting effective security control assessments. This publication allows agencies to customize these procedures and determine the appropriate level of depth and coverage to use in security control assessments.[73] According to NIST, agencies should consider various factors specific to the agency's information systems and the environments in which they operate in determining the assessment procedures to be performed and their level of depth and coverage. Such factors include the level of assurance needed from the assessment,[74] known threat and vulnerability information, and the agency's risk tolerance.

The reliability of security control assessments is critically important because the FDIC uses the results of the assessments to support a number of risk management activities. Such activities include identifying security weaknesses in information systems and the IT environment; prioritizing risk mitigation

[72] The FDIC plans to fully implement the CSAM tool by the third quarter of 2020.
[73] Depth refers to the rigor and level of detail involved in executing assessment procedures. Coverage refers to the scope or breadth of the assessment procedures.
[74] Information systems categorized as high or moderate generally require a greater level of assurance and, therefore, a greater level of depth and coverage than systems categorized as low.

activities; confirming the resolution of known security weaknesses; informing security authorization decisions; and supporting resource allocation decisions. For these reasons, the FDIC must ensure that it conducts security control assessments at an appropriate level of depth and coverage.

In January 2019, the FDIC OIG issued its report entitled, *Security Configuration Management of the Windows Server Operating System*.[75] The OIG's report identified instances that occurred in 2016 and 2017 in which contractor security control assessors did not perform assessment procedures at an appropriate level of depth and coverage. Specifically, the assessors did not test security control implementation, when warranted, and instead relied on narrative descriptions of the controls in FDIC policies, procedures, and system security plans and/or statements in interviews of FDIC or contractor personnel. As a result, the FDIC OIG determined that assessors did not have a basis to conclude on the effectiveness of the control activities they assessed. The OIG made two recommendations to the CIO to strengthen oversight of security control assessments conducted by contractors to ensure that they are conducted at an appropriate level of depth and coverage, and consistent with applicable requirements in contractual agreements.

In response, the OCISO, which has responsibility for overseeing the FDIC's security control assessments, engaged an outside firm independent of the security control assessors to review the sufficiency of their work. In addition, the OCISO assigned a reviewer to complete a Quality Assurance Checklist designed to ensure that security control assessments are consistent with applicable requirements and contractual agreements. Further, a Program Manager and management personnel within the OCISO must review and approve the checklist as an additional level of review. At the close of our audit, the FDIC OIG was reviewing the OCISO's process improvements and the manner in which the OCISO was implementing them to determine whether they were responsive to the OIG's recommendations.

***Preventing and Detecting Cyber Threats on the Network***

In November 2018, the FDIC engaged an external consulting firm to assess the effectiveness of its internal network security controls. As part of its assessment work, the consultant tested network security controls, including monitoring and logging processes, using techniques commonly associated with malicious threat actors. The consultant's report, which was issued in January 2019, stated that the FDIC's host and network-based monitoring controls detected the consultant's nefarious network traffic and attack patterns originating from Windows-based systems and generated actionable alerts to security operational personnel. [redacted]

We are not making any additional recommendations in this area.

[75] FDIC OIG AUD-19-004.

[76] [redacted]

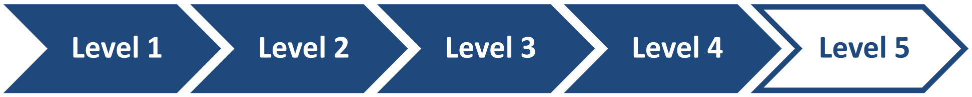
## RESPOND

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, Revision 2, *Computer Security Incident Handling Guide*,[77] 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 10: Maturity Rating – Incident Response**



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

The FDIC established policies, procedures, and guidelines for responding to computer security incidents; issued an agency-wide Incident Response Plan and Breach Response Plan; operated a centralized system to track and manage incidents; and implemented a CSIRT. Further, we performed selected tests of compliance with CSIRT's incident response and reporting procedures and found that the procedures were followed.

- We judgmentally selected 32 of 53 incidents recorded in the Combined Operational Risk, Security, Investigation, and Compliance Application (CORSICA)[78] between January 1, 2019 and May 31, 2019 and found that the FDIC:
  - Classified all 32 incidents consistent with the Attack Vectors Taxonomy defined by the United States Computer Emergency Readiness Team (US-CERT);[79] and
  - Resolved all 32 incidents within the timeframes prescribed in the CSIRT Standard Operating Procedures.

[77] NIST SP 800-61, Revision 2, (August 2012).
[78] CORSICA is the FDIC's system of record for tracking and managing incidents.
[79] 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. The 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, Revision 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.

- We judgmentally selected 11 of 18 incidents (from the universe of 53 incidents) recorded in CORSICA with an Event Type of “Data Loss Prevention” and confirmed that the FDIC reported all 11 incidents to US-CERT within prescribed timeframes.

We are not making recommendations in this area.

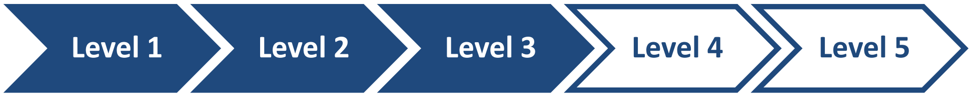
## Recover

The objective of the *Recover* function is to develop and implement activities to maintain plans for resilience and to restore any 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. This includes 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, Revision 1, *Contingency Planning Guide for Federal Information Systems*, dated May 2010, provides guidance on information system contingency planning activities.

**Figure 11: Maturity Rating – Contingency Planning**



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

The FDIC developed contingency planning policies, procedures, and plans. In addition, as of July 31, 2019, the FDIC was working to complete a multi-year Backup Data Center Migration Project. The purpose of this project is to remediate designated IT systems and applications supporting mission-essential functions to ensure they can be recovered within established timeframes and to migrate them to a new and expanded data center. The FDIC initiated the Backup Data Center Migration Project after it determined that it did not have the ability to rapidly restore its mission-essential systems and applications based on the results of its simulated exercises. Developing the new Backup Data Center was also intended to address the risk posed by the geographic proximity of the FDIC’s Backup Data Center to the FDIC’s primary data center.[80] Further, the new Backup Data Center has enhanced

[80] NIST SP 800-34, Revision 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). [redacted]

security capabilities, to allow security operations and other key security functions to be carried out without interruption in the event of a failure or other contingency at the primary data center.

As of July 31, 2019, the FDIC had migrated and successfully tested all but 2 of 23 mission-essential applications.[81] The FDIC was also working to decommission its IT equipment in the former backup site. When this work is completed, the FDIC will have greater assurance that it can maintain and restore mission-essential functions during an emergency within applicable timeframes.

We are not making recommendations in this area.

## 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 makes three new recommendations that, together with our prior-year recommendations, other OIG recommendations, and the FDIC's own information security initiatives, will strengthen the effectiveness of the FDIC's information security program controls and practices. The three recommendations are as follows:

- Reinforce to employees and contractor personnel the importance of properly safeguarding sensitive electronic and hardcopy information.
- Monitor employee and contractor compliance with policy requirements for properly safeguarding sensitive electronic and hardcopy information.
- Implement controls that ensure FDICLearn maintains accurate and complete information regarding user compliance with the FDIC's security and privacy awareness training requirement.

[81] [redacted]

# APPENDIX I – STATUS OF PRIOR-YEAR FISMA RECOMMENDATIONS

The following table summarizes our determinations regarding the status of previously unaddressed recommendations from the FISMA audit reports issued in 2015, 2016, 2017, and 2018.

| Recommendation | Status |
|---|---|
| **Report Issued in 2015, Recommendation 4**<br>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. | Open** |
| **Report Issued in 2016, Recommendation 5**<br>Review existing resource commitments and priorities for addressing Data Communications Plan of Action and Milestones (POA&Ms) and take appropriate steps to ensure they are addressed in a timely manner. | Open* |
| **Report Issued in 2017, Recommendation 4**<br>Develop a method and strategy for use by FDIC Divisions and Offices in the classification of risk ratings and risk profiles of corporate applications and systems. | Open |
| **Report Issued in 2017, Recommendation 5**<br>Develop and communicate the FDIC's information security risk tolerance level and risk profile used to prioritize risk mitigation activities. | Open |
| **Report Issued in 2017, Recommendation 6**<br>Develop an enterprise security architecture and integrate that architecture into corporate-wide enterprise architecture consistent with the Federal government's enterprise architecture requirements and the FDIC's business and mission requirements. | Closed |
| **Report Issued in 2017, Recommendation 9**<br>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. | Open** |
| **Report Issued in 2017, Recommendation 10**<br>Review and enhance the FDIC's vulnerability scanning processes to ensure that issues associated with conducting credentialed scans are resolved in a timely manner. | Open* |
| **Report Issued in 2017, Recommendation 15**<br>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. | Open* |
| **Report Issued in 2018, Recommendation 1**<br>Document descriptions of the FDIC's implementation of common controls (including both security and privacy controls) in a security plan or equivalent document. | Closed |
| **Report Issued in 2018, Recommendation 2**<br>Develop and implement procedures that define how the results of manual configuration reviews are used to assess compliance with approved baseline configurations. | Open* |

| Recommendation | Status |
|---|---|
| **Report Issued in 2018, Recommendation 3**<br>Revise the Infrastructure Configuration Management plan to define the types of interrelationships between configuration items that should be identified and where the information should be maintained. | Closed |
| **Report Issued in 2018, Recommendation 4**<br>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. | Open** |

* We informed Chief Information Officer Organization (CIOO) officials that we may not be able to evaluate corrective action closure packages provided to us after July 8, 2019 in order to meet the FISMA reporting deadline established by the Office of Management and Budget (OMB). Division of Finance Risk Management and Internal Controls (RMIC) provided us with a corrective action closure package for this recommendation on July 8, 2019. However, RMIC representatives stated that they were continuing to review the corrective actions for this recommendation and working with the CIOO to ensure it adequately addressed agreed-upon actions. As a matter of practice, RMIC reviews all corrective action closure packages before they are provided to the Office of Inspector General (OIG). The FDIC OIG plans to review this corrective action closure package after RMIC completes its work and is satisfied that the FDIC actions are sufficient to close the recommendation.

** RMIC completed its review and provided the corrective action closure package for this recommendation after July 8, 2019. The OIG is reviewing this corrective action closure package as part of its audit follow-up process.

# APPENDIX II – LIST OF ACRONYMS

| Acronym | Description |
|---|---|
| CHRIS-HR | Corporate Human Resources Information System-Human Resources |
| CIGIE | Council of the Inspectors General on Integrity and Efficiency |
| CIO | Chief Information Officer |
| CIOO | Chief Information Officer Organization |
| CISO | Chief Information Security Officer |
| CPO | Chief Privacy 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 |
| ERM | Enterprise Risk Management |
| FBDS | Failed Business Data Services |
| FDIC | Federal Deposit Insurance Corporation |
| FICAM | Federal Identity, Credential, and Access Management |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Modernization Act of 2014 |
| FY | Fiscal Year |
| GAO | U.S. Government Accountability Office |
| ICAM | Identity, Credential, and Access Management |
| IG | Inspector General |
| ISC-3 | Infrastructure Support Contract 3 |
| 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 the Chief Information Security Officer |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| PCM | Privacy Continuous Monitoring |
| PII | Personally Identifiable Information |
| PIV | Personal Identity Verification |
| POA&M | Plan of Action and Milestones |
| RADD | Regional Automated Document Distribution and Imaging System |
| 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 Report |
| SP | Special Publication |
| US-CERT | United States Computer Emergency Readiness Team |

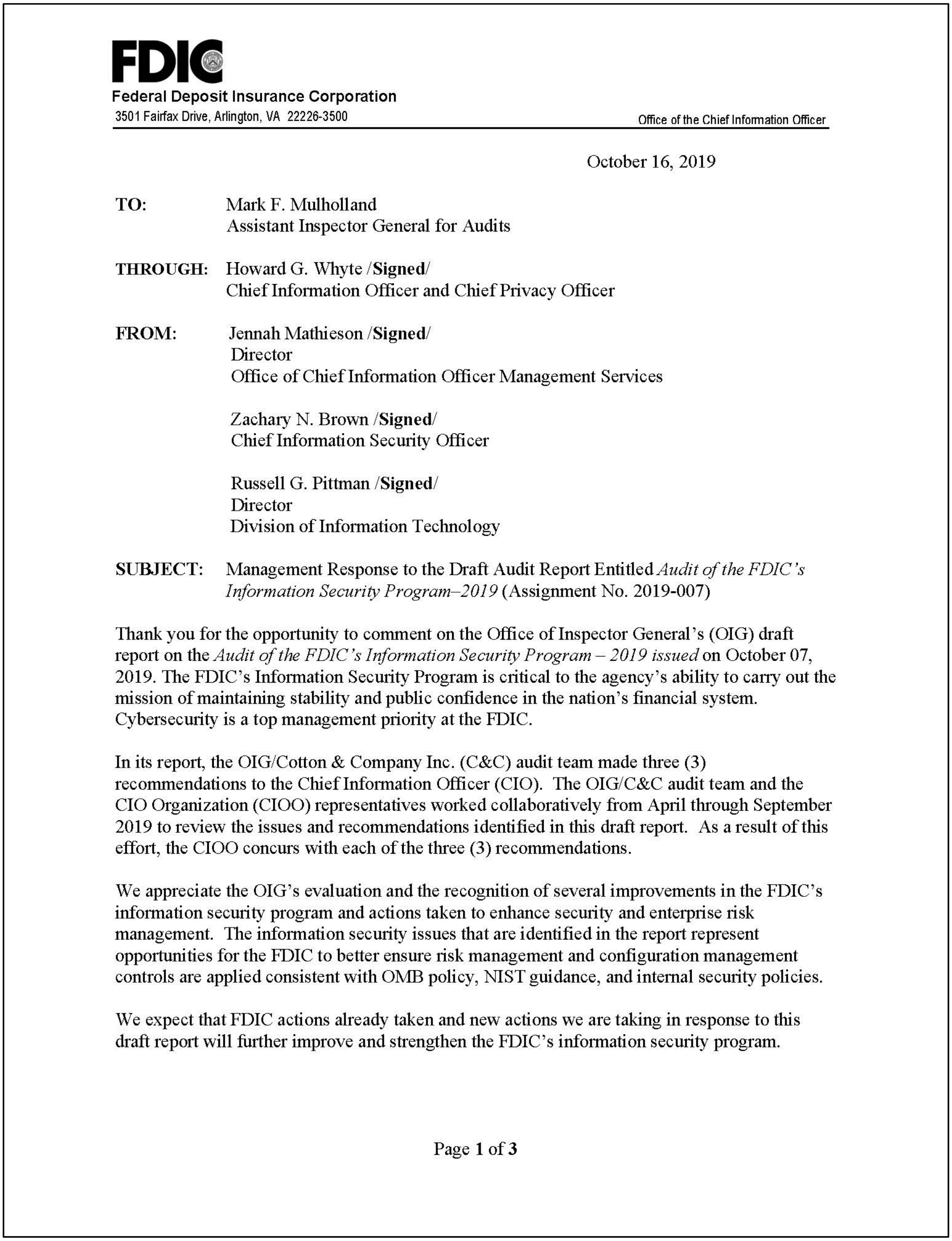
# Part II

☆☆☆☆☆☆☆☆

## FDIC Comments and OIG Evaluation

# FDIC Comments and OIG Evaluation

The FDIC's CIOO provided a written response, dated October 21, 2019, to a draft of the report. The response is presented in its entirety beginning on page II-2. In the response, CIOO officials concurred with all three 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-5.



FDIC

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226-3500

Office of the Chief Information Officer

October 16, 2019

**TO:** Mark F. Mulholland
Assistant Inspector General for Audits

**THROUGH:** Howard G. Whyte /**Signed**/
Chief Information Officer and Chief Privacy Officer

**FROM:** Jennah Mathieson /**Signed**/
Director
Office of Chief Information Officer Management Services

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

Russell G. Pittman /**Signed**/
Director
Division of Information Technology

**SUBJECT:** Management Response to the Draft Audit Report Entitled *Audit of the FDIC's Information Security Program–2019* (Assignment No. 2019-007)

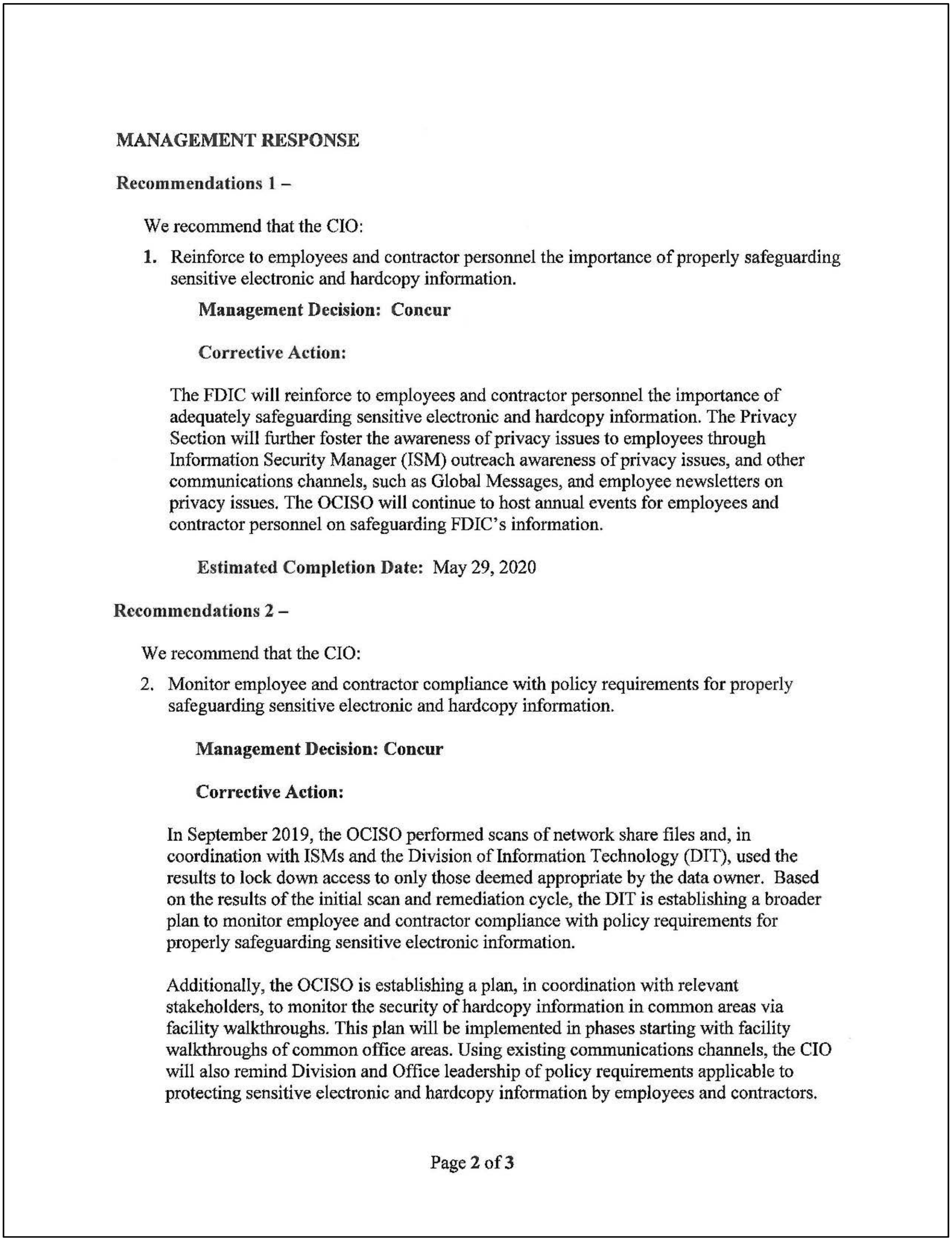
Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report on the *Audit of the FDIC's Information Security Program – 2019 issued* on October 07, 2019. The FDIC's Information Security Program is critical to the agency's ability to carry out the mission of maintaining stability and public confidence in the nation's financial system. Cybersecurity is a top management priority at the FDIC.

In its report, the OIG/Cotton & Company Inc. (C&C) audit team made three (3) recommendations to the Chief Information Officer (CIO). The OIG/C&C audit team and the CIO Organization (CIOO) representatives worked collaboratively from April through September 2019 to review the issues and recommendations identified in this draft report. As a result of this effort, the CIOO concurs with each of the three (3) recommendations.

We appreciate the OIG's evaluation and the recognition of several improvements in the FDIC's information security program and actions taken to enhance security and enterprise risk management. 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.

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

Page **1** of **3**



**MANAGEMENT RESPONSE**

**Recommendations 1 –**

We recommend that the CIO:

1. Reinforce to employees and contractor personnel the importance of properly safeguarding sensitive electronic and hardcopy information.

**Management Decision: Concur**

**Corrective Action:**

The FDIC will reinforce to employees and contractor personnel the importance of adequately safeguarding sensitive electronic and hardcopy information. The Privacy Section will further foster the awareness of privacy issues to employees through Information Security Manager (ISM) outreach awareness of privacy issues, and other communications channels, such as Global Messages, and employee newsletters on privacy issues. The OCISO will continue to host annual events for employees and contractor personnel on safeguarding FDIC's information.

**Estimated Completion Date:** May 29, 2020

**Recommendations 2 –**

We recommend that the CIO:

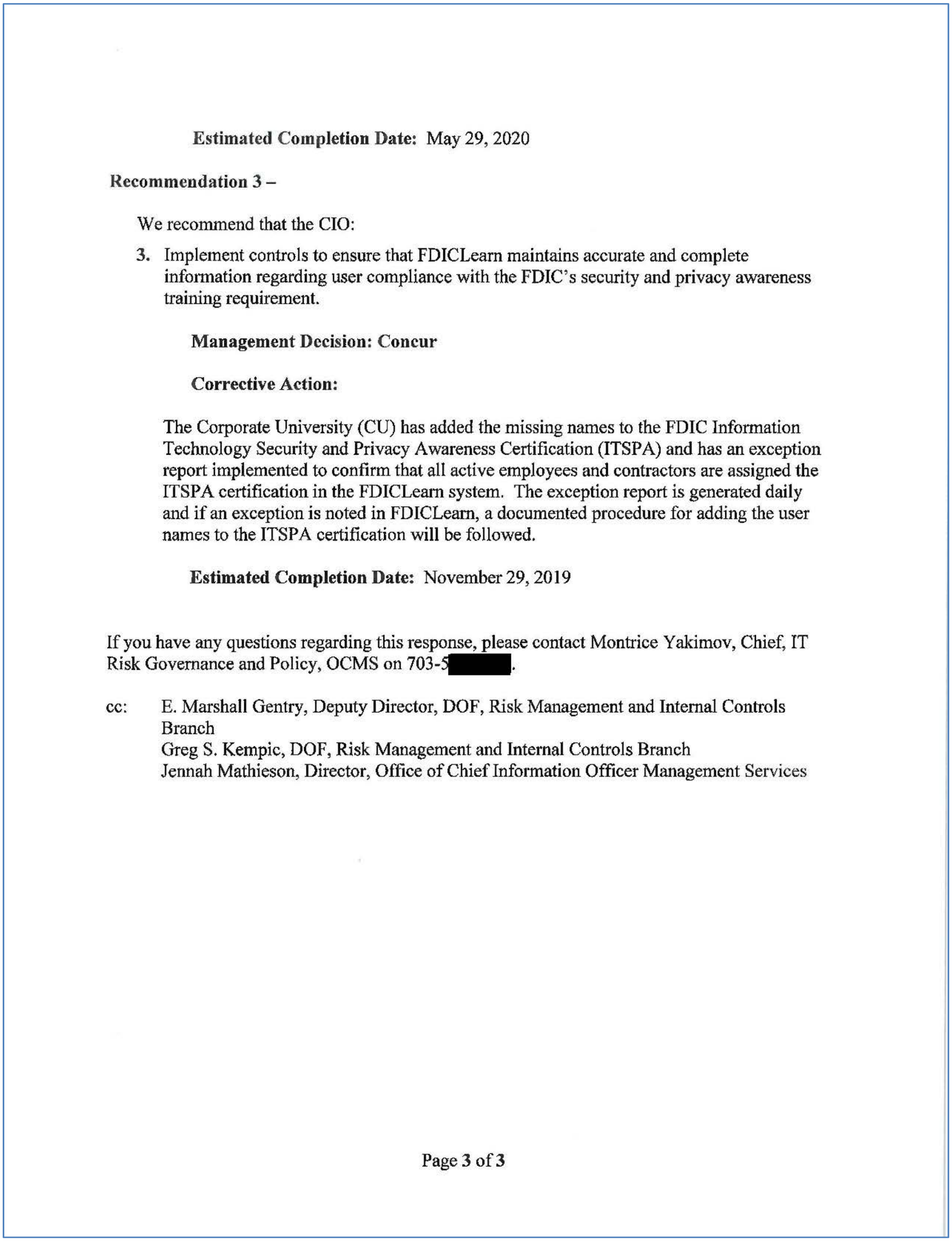
2. Monitor employee and contractor compliance with policy requirements for properly safeguarding sensitive electronic and hardcopy information.

**Management Decision: Concur**

**Corrective Action:**

In September 2019, the OCISO performed scans of network share files and, in coordination with ISMs and the Division of Information Technology (DIT), used the results to lock down access to only those deemed appropriate by the data owner. Based on the results of the initial scan and remediation cycle, the DIT is establishing a broader plan to monitor employee and contractor compliance with policy requirements for properly safeguarding sensitive electronic information.

Additionally, the OCISO is establishing a plan, in coordination with relevant stakeholders, to monitor the security of hardcopy information in common areas via facility walkthroughs. This plan will be implemented in phases starting with facility walkthroughs of common office areas. Using existing communications channels, the CIO will also remind Division and Office leadership of policy requirements applicable to protecting sensitive electronic and hardcopy information by employees and contractors.



**Estimated Completion Date:** May 29, 2020

**Recommendation 3 –**

We recommend that the CIO:

**3.** Implement controls to ensure that FDICLearn maintains accurate and complete information regarding user compliance with the FDIC's security and privacy awareness training requirement.

**Management Decision: Concur**

**Corrective Action:**

The Corporate University (CU) has added the missing names to the FDIC Information Technology Security and Privacy Awareness Certification (ITSPA) and has an exception report implemented to confirm that all active employees and contractors are assigned the ITSPA certification in the FDICLearn system. The exception report is generated daily and if an exception is noted in FDICLearn, a documented procedure for adding the user names to the ITSPA certification will be followed.

**Estimated Completion Date:** November 29, 2019

If you have any questions regarding this response, please contact Montrice Yakimov, Chief, IT Risk Governance and Policy, OCMS on 703-5[redacted].

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, Director, Office of Chief Information Officer Management Services

# Summary of the FDIC's Corrective Actions

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

| Rec No. | Corrective Action: Taken or Planned | Expected Completion Date | Monetary Benefits | Resolve:[a] Yes or No | Open or Close[b] |
|---|---|---|---|---|---|
| 1 | The FDIC will reinforce to employees and contractor personnel the importance of safeguarding sensitive electronic and hardcopy information. This will involve outreach by Division and Office ISMs, as well as communications through global messages, employee newsletters, annual events, and other channels. | May 29, 2020 | $0 | Yes | Open |
| 2 | The FDIC performed scans of its internal network shared drives in September 2019 and limited access to only those individuals deemed appropriate by data owners. Going forward, the FDIC will establish a plan to monitor compliance with policy requirements for safeguarding sensitive electronic information. The FDIC will establish a separate plan to monitor the security of hardcopy information in common areas via facility walkthroughs. Division and Office leadership will also be reminded of policy requirements for protecting sensitive electronic and hardcopy information. | May 29, 2020 | $0 | Yes | Open |
| 3 | The FDIC has addressed the individual exceptions identified during the audit. The FDIC has also begun generating a daily exception report to ensure that all active employees and contractors are scheduled to take security and privacy awareness training. If additional exceptions are identified, the FDIC will follow a written procedure to address them. | November 29, 2019 | $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.

| FDIC OIG website | Twitter | OVERSIGHT.GOV<br>ALL FEDERAL INSPECTOR GENERAL REPORTS IN ONE PLACE |
|---|---|---|
| www.fdicoig.gov | @FDIC_OIG | www.oversight.gov/ |