Security of Critical Building Services at FDIC-owned Facilities

March 2021 **AUD-21-003**

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.

Executive Summary

Security of Critical Building Services at FDIC-owned Facilities

The Federal Deposit Insurance Corporation (FDIC) relies heavily on critical building services to perform its mission-essential business functions and ensure the health and safety of its employees, contractors, and visitors. Critical building services include electrical power; heating, ventilation, and air conditioning (HVAC); and water. Threats to the uninterrupted delivery of these vital services can come from numerous sources, such as cyberattacks, malicious and accidental actions by trusted insiders, and environmental disasters.

In November 2014, the FDIC awarded a Consolidated Facilities Management Contract (Facilities Management Contract) to EMCOR Government Services, Inc. (EMCOR). Under the Facilities Management Contract, EMCOR operates, maintains, repairs, and replaces mechanical equipment that supports a wide range of critical building services at the FDIC's Virginia Square facility.

The audit objective was to assess whether the FDIC had effective controls and practices to protect electrical power, HVAC, and water services at its Virginia Square facility. The audit focused on security controls over three information systems used by the FDIC, EMCOR, and its subcontractors to monitor, manage, and help ensure the uninterrupted delivery of critical building services. The audit also assessed compliance with key security provisions in the Facilities Management Contract.

Results

The FDIC implemented various controls and practices to protect critical building services and ensure their continued delivery. For example, the FDIC required, and EMCOR implemented, a preventative maintenance program and routine inspections of critical building equipment and services to help ensure their safe and reliable operation. However, we found that the FDIC did not subject the three systems we reviewed to the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF), as required by Office of Management and Budget policy. As a result, we identified ineffective security controls for all three systems. For example, we identified weak account management practices, the use of unsupported vendor software, and a lack of security oversight and monitoring. Ineffective security controls and practices increased the risk of unauthorized access to these three systems, which could have led to a disruption of the systems, corruption of the systems' data, or other malicious activity.

The FDIC also did not maintain signed Confidentiality Agreements for EMCOR or its subcontractor personnel working at the Virginia Square facility, as required by the Facilities Management Contract and FDIC policy. These agreements are important to the security posture of the FDIC, because these personnel had access to the FDIC's information technology network and sensitive areas in the Virginia Square facility. In addition, the FDIC did not ensure that all EMCOR and subcontractor personnel had completed Information Security and Privacy Awareness Training or Insider Threat and Counterintelligence Awareness Training, as required by FDIC policy.

Recommendations

Our report contains 10 recommendations. We recommended that the FDIC include information systems that support critical building services within the FDIC's systems inventory, apply the NIST RMF to these systems, and modify the Facilities Management Contract to define security requirements for these systems. We also recommended that FDIC contractors and subcontractors execute Confidentiality Agreements and complete required Information Security and Privacy Awareness Training and Insider Threat and Counterintelligence Awareness Training. Finally, we recommended that the FDIC include a provision in its future contracts requiring contractor and subcontractor personnel to complete requisite training. The FDIC concurred with all 10 recommendations and plans to complete corrective actions by December 31, 2021.

Contents

March 29, 2021

Subject | ***Security of Critical Building Services at FDIC-owned Facilities***

The Federal Deposit Insurance Corporation (FDIC) relies heavily on critical building services to perform its mission-essential business functions and ensure the health and safety of its employees, contractors, and visitors. Critical building services include electrical power; heating, ventilation, and air conditioning (HVAC); and water. Threats to the uninterrupted delivery of these vital services can come from numerous sources, such as cyberattacks, malicious and accidental actions by trusted insiders, and environmental disasters.

In November 2019, a water main serving Arlington County, Virginia, ruptured, causing water pressure to drop at the FDIC's L. William Seidman Center (Virginia Square facility). This drop in water pressure required the FDIC to close its offices in the Virginia Square facility, displacing hundreds of employees and contractor personnel for one business day. The incident also caused the cooling systems that provide air conditioning to the FDIC's Primary Data Center in the Virginia Square facility to lose efficiency. Without adequate water pressure, the cooling systems will not work properly, making the Primary Data Center too hot for the information technology (IT) equipment to safely operate. To reduce heat output, the FDIC shut down its Development and Quality Assurance IT environments in the Primary Data Center and transferred certain IT systems to its Backup Data Center until water pressure was restored.

In June 2014, a contractor employee accidentally pressed the "Emergency Power Off" button in the Primary Data Center, terminating all electrical power to the IT equipment in the Primary Data Center. This accident damaged IT equipment, took mission-essential systems off-line, and required considerable effort to restore normal IT operations. These events underscore the need for proper controls to help ensure the security and continued delivery of critical building services.

The audit objective was to assess whether the FDIC had effective controls and practices to protect electrical power, HVAC, and water services at its Virginia Square facility. The audit focused on the effectiveness of security controls over the systems used by the FDIC and its contractors to monitor, manage, and help ensure the uninterrupted delivery of critical building services. The audit also assessed whether the FDIC ensured compliance with key security provisions in a major contract for managing building services at the Virginia Square facility.

We conducted this performance audit in accordance with generally accepted government auditing standards. Appendix 1 of this report provides additional details about our objective, scope, and methodology; Appendix 2 contains a list of acronyms and abbreviations; Appendix 3 contains an Advisory Memorandum that we issued to FDIC management addressing security concerns related to a system used to monitor critical building services and FDIC management's response; Appendix 4 contains a second Advisory Memorandum issued to FDIC management addressing potential security vulnerabilities that did not affect critical building services in the Virginia Square facility and FDIC management's response; and Appendix 5 and Appendix 6 contain the FDIC's comments on this report and a summary of the FDIC's corrective actions, respectively.

BACKGROUND

The FDIC's Division of Administration (DOA) has primary responsibility for managing critical building services at all FDIC-owned facilities. Building landlords have responsibility for managing critical building services at FDIC-leased facilities. The FDIC owns three facilities in the Washington, D.C., metropolitan area, and one facility in San Francisco, California. The largest and most complex of these FDIC-owned facilities is the Virginia Square facility. The Virginia Square facility consists of approximately 1.6 million gross square feet of office, conference, training, mechanical, and special use space (including a cafeteria, health unit, fitness center, and daycare center). The Virginia Square facility also houses a 354-room Student Residence Center; commercial businesses, including a credit union; and the FDIC's Primary Data Center that provides IT services for mission-essential business functions throughout the country.

In November 2014, the FDIC awarded a sizeable Consolidated Facilities Management Contract to EMCOR Government Services, Inc. (EMCOR), referred to as the "Facilities Management Contract." The Contract has a 3-year base term, two 2-year option periods, and a ceiling amount of $80.4 million. Under the Facilities Management Contract, EMCOR operates, maintains, repairs, and replaces mechanical equipment and systems that support a wide range of building services. Such building services include: electrical power, HVAC, fire alarm and sprinkler protection, pest control, elevator maintenance, and plumbing and water.

During the first quarter of 2020, EMCOR responded to 1,002 facility service calls[1] at FDIC-owned facilities in the Washington, D.C., area. EMCOR classified one of these service calls as an Emergency Call, 345 as Urgent Calls, and the remaining 656 as Routine Calls.[2]

As of April 2020, EMCOR had [redacted] personnel assigned to work on the Facilities Management Contract. [redacted] of these personnel worked in the Virginia Square facility, and the remaining [redacted] personnel worked in other FDIC-owned facilities. EMCOR also had agreements with more than [redacted] subcontractors that provided specialized facilities management support and expertise.

A Contracting Officer within DOA's Acquisition Services Branch has overall responsibility for administering the Facilities Management Contract. The Contracting Officer's responsibilities include ensuring that EMCOR complies with the terms and conditions of the Contract, and safeguarding the FDIC's business interests in the contractual relationship.

To assist with these responsibilities, the Contracting Officer appointed an employee within DOA's Corporate Services Branch, Facilities Operations Section, to serve as the Oversight Manager for the Facilities Management Contract. According to the Facilities Management Contract, the Oversight Manager's responsibilities include ensuring that EMCOR and its subcontractors satisfy the terms and conditions of the Contract and maintain satisfactory performance.

At the request of the Oversight Manager, the Contracting Officer also appointed three additional employees in DOA's Facilities Operations Section to serve as Technical Monitors who report to the Oversight Manager. According to the Facilities Management Contract, the Technical Monitors administer one or more functional areas and provide day-to-day oversight and monitoring of EMCOR's performance.

Systems Supporting Critical Building Services

Traditionally, organizations used stand-alone systems that were specifically designed to control, monitor, or manage vital functions such as electrical power, HVAC, and water.[3] These systems often required hands-on maintenance, such as adjusting

[1] DOA's *Award Term Plan Quarterly Service Request Response Totals* reports, dated March 17, 2020, and April 21, 2020, detail the number of facility service calls during the first quarter of 2020. The Facilities Management Contract defines three types of service calls: (1) *Emergency Calls* that pose "an immediate risk to health, safety, property, or the environment," such as an electrical power failure to a building, floor, or sensitive area (e.g., Chairman's Office); (2) *Urgent Calls* that require "quick intervention to prevent a worsening of the situation, "such as a power failure in an individual office or to non-critical equipment; and (3) *Routine Calls* that pose "little risk to health, life, property or the environment," such as unlocking a building occupant's office.
[2] Five hundred and fifty-one of the 1,002 service calls related to the Virginia Square facility. Of the 551 service calls, EMCOR classified 155 as Urgent and 396 as Routine.
[3] OIG analysis of the U.S. Department of Homeland Security's (DHS) report, entitled *Industrial Control Systems Assessments FY 2014 Overview and Analysis*, and the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-82, Rev. 2, *Guide to Industrial Control Systems (ICS) Security* (May 2015).

valves or flipping switches. Organizations relied primarily on physical security controls, such as guards, fences, and door locks to protect these systems. Over time, however, organizations began using wireless, mobile, and cloud-based applications to support remote access and other capabilities for these systems. While these changes introduced efficiency and functionality, they also increased the security risks associated with the systems.[4]

The FDIC, EMCOR, and its subcontractors use various types of information systems to monitor, manage, and help ensure the uninterrupted delivery of critical building services at the Virginia Square facility. Our audit covered three such systems:

- [redacted] EMCOR and FDIC personnel use [redacted] to monitor building mechanical equipment and services such as electric power distribution equipment; emergency electrical backup equipment; air handling and distribution systems; and water temperature and water pressure. [redacted] and sends text message alerts to wireless handheld devices used by EMCOR and FDIC personnel. These alerts provide information regarding the operation of critical equipment and services.[5]

- [redacted] EMCOR personnel use [redacted] to monitor and control HVAC services and equipment. [redacted] to allow EMCOR and its subcontractors to remotely monitor and control HVAC services and equipment.

- [redacted] FDIC and EMCOR personnel use [redacted] to: schedule and track preventative maintenance for mechanical equipment; track and manage facility service requests and work orders; maintain an inventory of mechanical equipment; and generate reports on the status of work activities, schedules, repair history, and planned and completed preventive maintenance. In addition, the FDIC uses data in [redacted] to evaluate EMCOR's performance under the Facilities Management Contract. [redacted] that FDIC employees and EMCOR personnel [redacted].

The Facilities Management Contract requires EMCOR to work with the vendors of [redacted] and [redacted] to continually evaluate the systems for effectiveness and upgrade them for the benefit of building operations. Such upgrades include implementing software patches, revisions, and bug fixes to maintain system operations. The Facilities Management Contract also requires EMCOR to provide IT

[4] According to NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013), information system-related security risks "are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation."

[5] For example, [redacted] monitors building water pressure, which is critical to the proper operation of the systems that cool the Primary Data Center. If [redacted] detects a change in water pressure that falls outside of normal parameters, [redacted] notifies EMCOR and FDIC personnel via a text message.

support and troubleshooting for [redacted]. DOA personnel stated that EMCOR and its subcontractors maintain [redacted], and [redacted] separate from the FDIC's IT network.

The Facilities Management Contract states that EMCOR will "implement adequate administrative, technical, physical, and procedural security controls to ensure that all FDIC information in its possession or under its control is adequately protected from loss, misuse, and unauthorized access or modification." However, the Facilities Management Contract does not define specific security requirements for the systems used by EMCOR to monitor, manage, or control critical building services, including [redacted], and [redacted].

Federal Statutes, Policies, and Guidelines

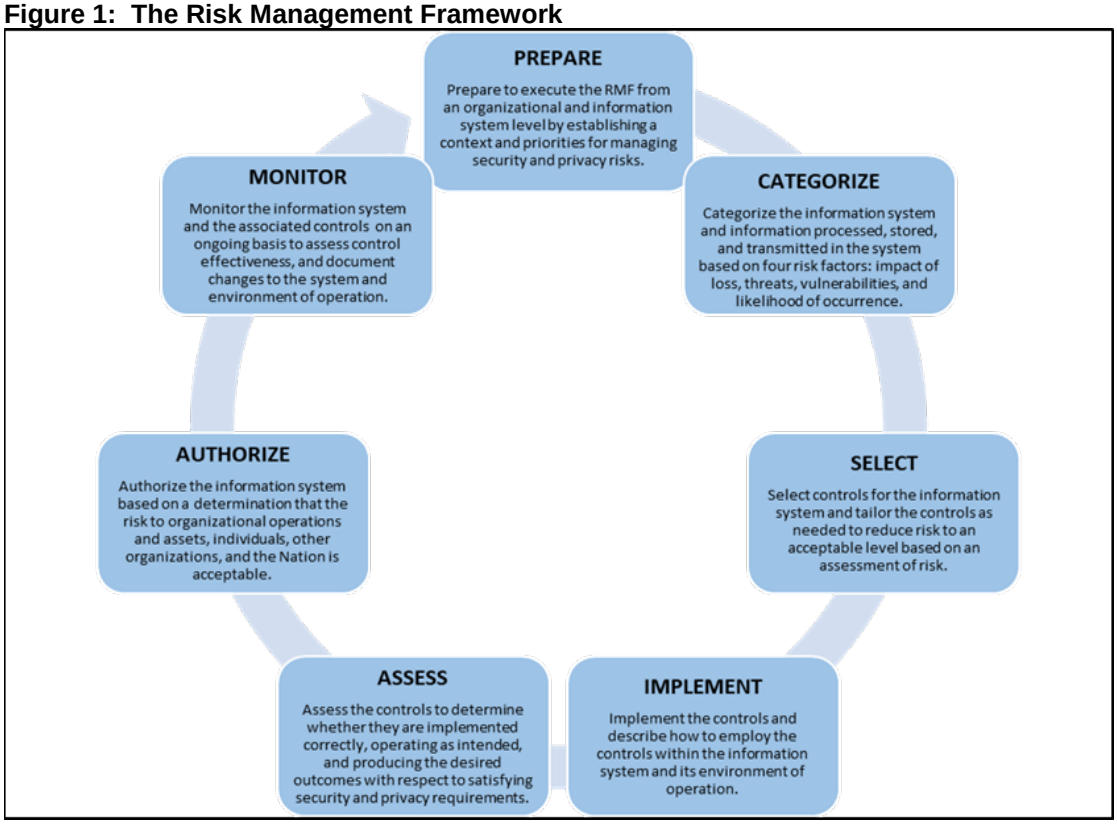
The Federal Information Security Modernization Act of 2014 (FISMA)[6] requires Federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems. According to the statute, this requirement extends to "information systems that support the operations and assets of the agency, 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 standards are issued in the form of Federal Information Processing Standards (FIPS) publications and recommended guidance within NIST Special Publications (SP). NIST FIPS and SPs provide Federal agencies with a framework for developing appropriate controls over the confidentiality, integrity, and availability of their information and information systems.

The Office of Management and Budget's Circular No. A-130, *Managing Information as a Strategic Resource* (OMB Circular A-130),[7] requires Federal agencies to apply NIST FIPS and SPs to protect their information systems. NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations*,[8] establishes a Risk Management Framework (RMF) that Federal agencies must use to manage the security and privacy risks associated with their information systems. According to NIST SP 800-37, Rev. 2, the RMF is designed to be technology neutral so that agencies can apply it to any type of information system without modification.[9]

[6] Pub. L. No. 113-283 (December 2014), codified at 44 U.S.C. § 3554 *et seq*. The FDIC has determined that FISMA is legally binding on the FDIC.
[7] OMB Circular A-130, *Managing Information as a Strategic Resource* (July 2016). The FDIC has determined that OMB Circular A-130 is "generally applicable" to the FDIC, to the extent that the Circular aligns with OMB's statutory authorities, does not impose obligations on the FDIC based on statutes that are legally inapplicable to the FDIC, and does not conflict with the FDIC's independence, statutory obligations, or regulatory authority. FDIC Review of OMB Circular A-130 (July 28, 2016).
[8] NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations* (December 2018). This publication superseded NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (February 2010).
[9] NIST SP 800-37, Rev. 2, states that the RMF applies to cloud-based systems, industrial/process control systems, building automation systems, weapons systems, cyber-physical systems, applications, Internet of Things (IoT) devices, and mobile devices/systems.

NIST SP 800-37, Rev. 2, states that agencies should tailor system security controls and implementation details using the RMF. Figure 1 illustrates the seven life cycle steps of the RMF.

Figure 1: The Risk Management Framework



Source: Office of Inspector General (OIG) analysis of NIST SP 800-37, Rev. 2.

NIST SP 800-82, Rev. 2, *Guide to Industrial Control Systems (ICS) Security* (May 2015), provides agencies with guidance on how to apply the RMF to industrial control systems, which are a type of Operational Technology (OT) system. NIST SP 800-37, Rev. 2, defines OT systems as "programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms." [redacted] and [redacted] are OT systems.

According to NIST SP 800-82, Rev. 2, OT systems have characteristics that differ from traditional information processing systems. For example, OT systems often use specialized hardware and software that must be managed by engineers with specific skill sets, experience, and expertise. NIST 800-82 also states that OT systems may not have IT security capabilities commonly found in traditional IT systems, such as encryption or error logging.

NIST SP 800-82, Rev. 2, presents a set of security controls that agencies can customize and tailor for their OT systems. These controls are based on the security controls defined in NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.[10]

Under FISMA, the FDIC's Chief Information Security Officer (CISO) has primary responsibility for planning, developing, and implementing an information security program that supports the mission of the FDIC. Such responsibility includes establishing processes to implement the RMF for all information systems within the FDIC. The CISO reports directly to the FDIC's Chief Information Officer.

AUDIT RESULTS

The FDIC implemented various controls and practices to protect critical building services and ensure their continued delivery. For example, the FDIC required, and EMCOR implemented, a preventative maintenance program and routine daily inspections of critical building equipment and services to help ensure their safe and reliable operation. EMCOR's inspections included checking temperature and humidity readings in the Primary Data Center. In addition, the FDIC conducted after action reviews of incidents involving critical building services to identify needed security control improvements.

However, we found that the FDIC did not subject [redacted], or [redacted] to the NIST RMF as required by OMB policy. As a result, we identified ineffective security controls for all three systems, including weak account management practices, the use of unsupported vendor software, and a lack of security oversight and monitoring. Ineffective security controls and practices increased the risk of unauthorized access to these systems, which could have led to a disruption of the systems, corruption of the systems' data, or other malicious activity.

The FDIC also did not maintain signed Confidentiality Agreements for EMCOR or its subcontractor personnel who worked in the Virginia Square facility. Both the Facilities Management Contract and FDIC policy required EMCOR and its subcontractor personnel to sign a Confidentiality Agreement because these personnel had access to the FDIC's IT network and/or sensitive areas in the Virginia Square facility. In addition, the FDIC did not ensure that all EMCOR and subcontractor personnel completed required Security and Privacy Awareness Training or Insider Threat and Counterintelligence Training.

[10] NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013), provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations, assets, individuals, other organizations, and the Nation from a diverse set of threats, including hostile cyberattacks, natural disasters, structural failures, and human errors.

Systems Not Subject to the RMF

OMB Circular A-130 requires Federal agencies to use the RMF defined in NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations*, to protect their information systems. The RMF involves creating a systems inventory; categorizing systems based on risk; selecting, tailoring, and implementing system controls; assessing control effectiveness; authorizing systems to operate; and performing continuous monitoring. NIST SPs 800-37, Rev. 2, and 800-82, Rev. 2, provide guidance on how agencies can tailor the RMF for OT systems, such as [redacted] and [redacted].

The FDIC did not subject [redacted], or [redacted] to the RMF. As a result, all three systems had security control vulnerabilities that, if exploited, could have led to a security incident.[11]

Systems Not in the Systems Inventory

FISMA requires Federal agencies to maintain an inventory of all information systems operated by or under the control of the agency. However, the FDIC did not include [redacted], or [redacted] in its centralized systems inventory.

According to NIST SP 800-37, Rev. 2, establishing and maintaining a comprehensive system inventory is a fundamental step in effectively implementing the RMF. NIST SP 800-37, Rev. 2, states that the system inventory "serves to inform the governing organization of plans to develop the system or the existence of the system; the key characteristics of the system; and the expected security and privacy implications for the organization due to the operation and use of the system." Unless the FDIC includes [redacted], and [redacted] in the systems inventory, the Office of the Chief Information Security Officer (OCISO) has limited assurance that security risks are properly identified and addressed.

System Security Controls Not Defined or Monitored

Because the FDIC did not subject [redacted], or [redacted] to the RMF, the FDIC had not categorized these systems based on an assessment of risk.[12] In addition, neither the FDIC nor EMCOR developed a security plan that documented the selection, tailoring, and implementation of security controls for the systems. OMB Circular No. A-130 requires Federal agencies to develop system security plans that

[11] We reviewed a listing of all FDIC computer security incidents covering the period October 1, 2019 through January 28, 2021 recorded in the Combined Operational Risk, Security, Investigation, and Compliance Application—the FDIC's system of record for tracking and managing security incidents—and found no incidents involving [redacted], or [redacted].

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

document the security requirements for their systems and the security controls in place or planned for meeting those requirements. The FDIC also did not assess the effectiveness of security controls for [redacted], or [redacted], nor did it continuously monitor security controls for these systems.

In March 2015, DOA modified the Facilities Management Contract to remove a standard clause requiring EMCOR and its subcontractors to comply with NIST security standards and guidelines, including the RMF.[13] A representative of DOA stated that the clause was removed, because [redacted] was not connected to the FDIC's IT network and, therefore, NIST security standards and guidelines did not apply to [redacted].[14] However, DOA did not consult with the OCISO on the decision to remove the security clause. Removing the clause meant that EMCOR was no longer obligated to adhere to NIST security standards and guidelines for any of the systems referenced in the Facilities Management Contract, including [redacted], and [redacted].

The applicability of NIST security standards and guidance to an information system is not based on whether the system is connected to the agency's IT network. The OMB policy requirement to apply the RMF extends to all "information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source." This includes information systems that do not interface with agency IT networks. Without the clause, the Facilities Management Contract does not define clear roles and responsibilities for the FDIC and EMCOR in ensuring the security of information systems used to manage critical building services. NIST SP 800-37, Rev. 2, recommends that agencies address security and privacy requirements for external providers in agency contracts.

Systems Were Vulnerable

Because the FDIC did not subject [redacted], or [redacted] to the RMF, all three systems had security vulnerabilities that placed the systems and the underlying data at risk.

[redacted]

On March 20, 2020, we issued an Advisory Memorandum to the former Deputy to the Chairman and Chief Operating Officer (COO)[15] and the CISO describing the

[13] The FDIC removed Section 7.4.2-1, *Security and Privacy Compliance for IT Services*, of the Facilities Management Contract.
[14] DOA did not consider the security requirements of other systems, such as [redacted] and [redacted], when deciding to remove the security clause from the Facilities Management Contract.
[15] Effective January 19, 2021, the individual serving as the COO transitioned to a different role in the FDIC as the Deputy to the Chairman for External Affairs. On this same date, the individual serving as the Deputy to the Chairman and Chief of Staff assumed the responsibilities of the COO.

following potential security vulnerabilities associated with an [redacted] server[16] supporting [redacted].

- The [redacted] server was running an obsolete [redacted]. NIST SP 800-53, Rev. 4, recommends that agencies replace system components when support is no longer available from the developer, vendor, or manufacturer. [redacted]

- The [redacted] server had two potentially vulnerable IT services enabled: [redacted]

- Neither the FDIC nor EMCOR had reviewed the security event logs on the [redacted] server since it had been installed. NIST SP 800-53, Rev. 4, recommends that organizations review and analyze system event logs for indications of inappropriate or unusual activity, including cyberattacks.

- The [redacted] server stored a password in an unencrypted (plaintext) format.[20] NIST SP 800-53, Rev. 4, recommends that organizations store passwords in an encrypted format to reduce the risk of a malicious actor compromising the passwords for unauthorized activity.

A copy of the Advisory Memorandum is included in Appendix 3 of this report.

In a written response to our Advisory Memorandum, the former FDIC Deputy to the Chairman and COO and the CISO stated that [redacted] does not reside on the FDIC

[16] According to NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems* (August 2002), a server is a computer or device on a network that manages network resources. Examples include Web servers that store, process, and deliver Web pages, and database servers that store data and process queries.

[17] [redacted]

[18] [redacted]

[19] [redacted]

[20] Encryption is a process that changes plaintext information (data that can be read) into ciphertext (data in an encrypted format).

network.[21] However, management's response acknowledged that these security vulnerabilities presented several risks. For example, the former Deputy to the Chairman and COO and the CISO stated in their response that:

- A [redacted] on [redacted] could interrupt data used to monitor building systems (to the extent facilities personnel are unable to monitor the systems manually);
- A cyberattack could interrupt updates and maintenance of the [redacted]r server; and
- If an adversary were able to use [redacted] as [redacted], the contractual relationship between the vendor and the FDIC could create a reputational risk to the FDIC.

DOA staff stated that EMCOR installed a firewall on July 9, 2020 to protect the [redacted] server from cyberattacks.[22] Further, DOA staff stated that the vendor had [redacted] In addition, the OCISO conducted a forensic review of the security event log for the [redacted] server. The forensic review found that the security event log contained numerous security events covering a 2-day period. According to the review, the majority of events in the log consisted of [redacted] OCISO staff stated that they had found no evidence of unauthorized access to the [redacted] server based on their review of the server event log.

The FDIC decided not to upgrade the obsolete [redacted]. According to DOA staff, upgrading the obsolete [redacted] would also require that the FDIC [redacted]. At the close of our audit field work, the OCISO was assessing whether the FDIC could obtain [redacted].

In addition to the actions taken during the audit to strengthen the security posture of [redacted], DOA officials stated that EMCOR's inspections of critical building equipment each day help to mitigate the risk of an outage of [redacted]. In addition, Chief Information Officer Organization (CIOO) officials stated that server administrators electronically monitor the temperature of servers in the Primary Data Center. If the temperature of these servers rose above established thresholds, alerts would be sent to the server administrators, who in turn could notify DOA.[23] Nevertheless, EMCOR's inspections of critical building equipment and the CIOO's monitoring of servers in the Primary Data Center would not mitigate the security

[21] The FDIC's response to our Advisory Memorandum is contained in Appendix 3 of this report.
[22] We did not assess the effectiveness of the firewall in protecting the [redacted] server as part of the audit.
[23] An assessment of the CIOO's monitoring of the servers in the Primary Data Center was not within the scope of the audit.

vulnerabilities that placed the [redacted] server at risk of becoming potentially compromised. In addition, EMCOR's inspections and the CIOO's monitoring of servers do not provide for real-time monitoring of all critical building equipment covered by [redacted]. The absence of such monitoring could delay the identification of, and response to, facilities-related issues.

[redacted] and [redacted]

We identified the following weaknesses with respect to account management practices:

- Users of [redacted]. NIST SP 800-53, Rev. 4, recommends that organizations [redacted] for their information system accounts on [redacted] create an elevated risk that malicious actors could compromise system accounts.

- [redacted] under the Facilities Management Contract as of February 2020. NIST SP 800-53, Rev. 4, recommends that organizations [redacted] increases the risk that the accounts will be used for unauthorized or malicious activity.

- [redacted] NIST SP 800-53, Rev. 4, recommends that agencies [redacted] should be commensurate with the risk associated with the .[24] [redacted] presented an elevated risk of unauthorized access to , because the system is [redacted]

[24] For example, FDIC Policy [redacted].

In addition, at the start of our audit, we noted that the FDIC was using an outdated version of [redacted].[25] As a result, the FDIC was not receiving security patches or fixes for [redacted] at that time. According to the vendor's public website, the version of [redacted] used by the FDIC had a number of known security vulnerabilities that, if exploited, could impact the availability of [redacted] and allow for unauthorized access or other malicious activities.[26] EMCOR staff asserted that the risk associated with these vulnerabilities was mitigated, because the subcontractor that supports and services [redacted] for the FDIC had implemented supplemental security controls. Assessing the effectiveness of the subcontractor's supplemental security controls was not within the scope of this audit. However, as previously stated, NIST recommends that organizations use up-to-date and vendor-supported software to mitigate the risk of a malicious actor exploiting known vulnerabilities. In October 2019, DOA upgraded [redacted] to a current and supported version of the software.[27]

In our FISMA audit report issued in October 2020, we reported that the FDIC had not properly categorized some of its outsourced information systems or subjected these systems to a risk assessment, authorization to operate, or ongoing monitoring as defined in the RMF.[28] We recommended in our FISMA audit report that the FDIC implement a process to ensure that its outsourced systems are subject to the RMF. The FDIC expects to complete corrective action by December 2021. Until the FDIC subjects all of its information systems (including systems used to support critical building services) to the RMF, the FDIC cannot be sure that it will identify and address security risks in a timely manner. The FDIC has captured this risk in its Risk Inventory for the agency.

Recommendations

We recommend that the CISO:

1. Include systems supporting critical building services in FDIC-owned facilities in the FDIC's systems inventory.

2. Implement the NIST Risk Management Framework for systems supporting critical building services.

We recommend that the Deputy to the Chairman and Chief of Staff and COO:

3. Modify the Facilities Management Contract to define security requirements for systems that support critical building services in FDIC-owned facilities.

[25] [redacted]
[26] [redacted]
[27] [redacted]
[28] OIG Report, *The FDIC's Information Security Program–2020* (FDIC OIG AUD-21-001) (October 2020).

Confidentiality Agreements Not Executed or Maintained

The Facilities Management Contract requires all EMCOR and subcontractor personnel with access to FDIC facilities, networks, and/or information systems, or sensitive information (whether in hardcopy or electronic form) to execute a Confidentiality Agreement. The Facilities Management Contract states that personnel with such access who do not sign a Confidentiality Agreement are prohibited from conducting work at the FDIC. Confidentiality Agreements serve as a key control for mitigating the risk of unauthorized disclosure of sensitive information, and for holding individuals accountable for non-compliance with FDIC security requirements. The FDIC's Acquisition Policy Manual directs contracting personnel to maintain Confidentiality Agreements in the FDIC's official contract file—the Contract Electronic File (CEFile).[29]

As of June 2020, [redacted] EMCOR and subcontractor personnel[30] assigned to the Facilities Management Contract had broad unescorted access to the Virginia Square facility, including restricted areas such as building mechanical equipment rooms. In addition, [redacted] (43 percent) EMCOR personnel had access to certain systems, such as email, on the FDIC's IT network.[31] Due to the sensitivity of the information and assets that EMCOR and its subcontractors have access to, 86 percent of EMCOR and subcontractor personnel ([redacted] individuals) served in positions that the FDIC designated as either Moderate or High Risk.[32]

During the course of our audit, FDIC contracting officials could not verify that the [redacted] EMCOR and [redacted] subcontractor personnel had completed Confidentiality Agreements. The Facilities Management Contract required such agreements for all of them; however, FDIC contracting officials could not locate copies of these agreements. Since the time that the OIG brought this to the attention of DOA personnel, [redacted] EMCOR employees have now completed the Confidentiality Agreements. The FDIC's collection of such Agreements from subcontractor personnel was still in progress at the close of our audit.

The lack of signed Confidentiality Agreements was not isolated to the Facilities Management Contract. Since 2006, we have reported several instances in which the FDIC did not consistently execute or maintain Confidentiality Agreements for its contractor and subcontractor personnel that handle sensitive information and provide critical services.

[29] The CEFile contains pre-award, post-award, and oversight management contract documentation.
[30] This consists of [redacted] EMCOR employees and [redacted] subcontractor personnel.
[31] None of EMCOR's [redacted] subcontractor personnel had access to the FDIC IT network.
[32] FDIC Directive 1610.2, *Personnel Security and Suitability Program for Contractors and Contractor Personnel* (January 2020), states that the FDIC assigns risk level designations to contractor personnel based on their job category or areas of functional respons bility. The FDIC assigns contractor personnel to 1 of 4 risk levels: Low, Moderate, High, or High IT. Moderate Risk positions involve duties reflecting the potential for moderate to serious impact to the FDIC's mission, integrity, or efficiency. High Risk positions involve duties reflecting the potential for exceptionally serious impact to the FDIC's mission, integrity, or efficiency.

- In January 2006, we reported that the FDIC did not maintain signed Confidentiality Agreements for 92 percent of the contracts reviewed (12 of 13 contracts).[33] These contracts involved access to human resources information, such as employee benefits, and finance information. We recommended that the FDIC require contractors to sign Confidentiality Agreements.

- In September 2008, we reported that the FDIC did not maintain Confidentiality Agreements for 30 percent of the contractor personnel reviewed (14 of 46 individuals).[34] These contractor personnel provided support for bank resolution and receivership activities. We recommended that the FDIC develop a control mechanism to ensure that Contracting Officers obtain signed Confidentiality Agreements from contractor personnel.

- In October 2012, we reported that the FDIC did not consistently execute and maintain Confidentiality Agreements for contractor and subcontractor personnel with access to sensitive failed bank data.[35] We recommended that the FDIC review all contractor and subcontractor employees assigned to the contract and execute Confidentiality Agreements. We also recommended that the FDIC enhance controls designed to ensure that Confidentiality Agreements are executed and maintained.

- In September 2017, we reported that the FDIC could not locate signed Confidentiality Agreements in the CEFile for 75 percent of separated contractor personnel (36 of 48 individuals).[36] We made a series of recommendations to improve the FDIC's controls for mitigating the risk of unauthorized access to, and inappropriate removal and disclosure of, sensitive information by separating personnel.

While the FDIC indicated that it had previously taken actions to address these findings reported above, the FDIC's actions have proven to be ineffective.[37]

The Contracting Officer and Oversight Manager explained that turnover in personnel was a contributing factor for the lack of signed Confidentiality Agreements. In addition, the Contracting Officer stated that the FDIC had not established an effective control to ensure that contractor and subcontractor personnel sign Confidentiality

[33] OIG Report, *FDIC Safeguards Over Personal Employee Information* (FDIC OIG EVAL-06-005) (January 2006).
[34] OIG Report, *Protection of Resolution and Receivership Data Managed or Maintained by an FDIC Contractor* (FDIC OIG AUD-08-015) (September 2008).
[35] OIG Report, *Invoices Submitted by Lockheed Martin Services, Inc. under the FDIC's Data Management Services Contract* (FDIC OIG AUD-13-002) (October 2012).
[36] OIG Report, *Controls over Separating Personnel's Access to Sensitive Information* (FDIC OIG EVAL-17-007) (September 2017).
[37] In 2017, the OIG updated its procedures to ensure that we review the corrective actions undertaken by the FDIC before we close each recommendation. The procedures now include a review by our office of all recommendations to ensure that the FDIC's actions are responsive and sufficient to satisfy the recommendations.

Agreements, particularly when contractors add personnel after the initial contract award.

The FDIC relies on Confidentiality Agreements to inform contractor personnel of their obligation to properly handle and safeguard sensitive information, and to hold accountable those personnel who fail to meet that obligation. Further, without signed Confidentiality Agreements, the FDIC has reduced assurance that contractor personnel will understand their responsibilities for protecting the confidentiality, integrity, and availability of sensitive information. In addition, the FDIC may face difficulties in pursuing appropriate remedies against contractor or subcontractor personnel who fail to handle or safeguard sensitive FDIC information and assets. Absent signed Confidentiality Agreements, the FDIC is at increased risk of an unauthorized disclosure of sensitive information.

Recommendations

We recommend that the Deputy to the Chairman and Chief of Staff and COO:

4. Obtain completed Confidentiality Agreements for all EMCOR and subcontractor personnel required to execute such agreements under the Facilities Management Contract, and maintain copies in the FDIC's contracting files.

5. Ensure that Oversight Managers assigned to other FDIC contracts have obtained signed Confidentiality Agreements for all contractor and subcontractor personnel required to sign such agreements.

6. Provide training to Oversight Managers to ensure that Confidentiality Agreements are consistently executed and maintained as required by FDIC policy.

Mandatory Training Not Completed

The majority of EMCOR and subcontractor personnel assigned to work at the Virginia Square facility did not complete mandatory Information Security and Privacy Awareness Training, or Insider Threat and Counterintelligence Awareness Training. This weakness increased the risk of a security incident, such as a breach,[38] or an insider threat not being timely detected or reported.

[38] OMB defines the term "breach" as a type of security incident that involves the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose. A breach can be inadvertent, such as a loss of hard copy documents or portable electronic storage media, or deliberate, such as a successful cyberattack by a hacker, criminal, or other adversary.

Security and Privacy Awareness Training

The Facilities Management Contract requires EMCOR and its subcontractors to comply with FDIC Directive 1360.9, *Protecting Sensitive Information* (April 2007). FDIC Directive 1360.9 states that all contractor personnel with access to sensitive hardcopy or electronic information must complete the FDIC's Information Security and Privacy Awareness Training.[39] Such training is intended to inform personnel of the information security risks associated with their activities and their responsibility to comply with FDIC policies and procedures designed to reduce these risks. The Facilities Management Contract states that contractor personnel who do not have access to the FDIC's network and, therefore, cannot access the on-line version of the training, must obtain the training materials through other digital means and provide written confirmation of completion to the Oversight Manager.

As of April 2020, only 37 percent of EMCOR personnel with unescorted access to the Virginia Square facility had completed the FDIC's Information Security and Privacy Awareness Training within the last year (EMCOR personnel). Of the personnel that had not completed this training, did not have access to the FDIC's IT network. Further, as of June 2020, none of the subcontractor personnel with unescorted access in the Virginia Square facility had completed the required Information Security and Privacy Awareness Training; none of these individuals had access to the FDIC's IT network.

These exceptions occurred because the Oversight Manager was unaware of the requirements in the Facilities Management Contract and FDIC Directive 1360.9 for all personnel to complete the Information Security and Privacy Awareness Training, even if they do not have access to the FDIC's IT network.[40] Following our inquiries, the FDIC required all EMCOR personnel to complete the Information Security and Privacy Awareness Training. As of July 2020, all EMCOR personnel had completed the training. Based on documentation provided to us by EMCOR, 42 percent of subcontractor personnel had completed the training (subcontractor personnel) as of September 11, 2020.

Insider Threat and Counterintelligence Awareness Training

FDIC Directive 1600.7, *FDIC Insider Threat and Counterintelligence Program* (September 2016),[41] requires all persons employed by, contracted to, or detailed or

[39] FDIC Circular 1360.16, *Mandatory Information Security Awareness Training* (July 2002), states that the mandatory awareness training must be completed within 5 working days of receiving a network ID, and annually thereafter.
[40] In our FISMA audit report issued in October 2020, we reported that the FDIC had implemented effective controls for ensuring that users of the FDIC's IT network completed the required Information Security and Privacy Awareness Training.
[41] FDIC Directive 1600.7, *FDIC Insider Threat and Counterintelligence Program* (September 2016). The FDIC Insider Threat and Counterintelligence Program provides an integrated framework for FDIC personnel to affirmatively protect the FDIC using a defensive program to address internal and external threats and risks posed to its personnel, facilities, assets, resources, and classified and sensitive information, by insider threats and foreign entities.

assigned to the FDIC, to complete Insider Threat and Counterintelligence Awareness Training within 30 days of employment, and annually thereafter. This requirement covers contractor and subcontractor personnel whose business location is primarily within FDIC spaces; who have unescorted access to FDIC facilities; or who have access to the FDIC's IT network. FDIC Directive 1600.7 states that all personnel have a responsibility to protect the FDIC by observing and reporting activities that could pose risks to the FDIC's mission and assets.

Again, only 37 percent of the EMCOR personnel with unescorted access to the Virginia Square facility completed the Insider Threat and Counterintelligence Awareness Training ([redacted] EMCOR personnel). Of the [redacted] EMCOR personnel who did not complete this training, [redacted] did not have access to the FDIC's IT network.

In addition, none of the [redacted] EMCOR subcontractor personnel with unescorted access to the Virginia Square facility completed the Insider Threat and Counterintelligence Awareness Training. These [redacted] subcontractor personnel did not have access to the FDIC's IT network. In response to our inquiry, the Oversight Manager worked with EMCOR to ensure that the EMCOR personnel completed the Insider Threat and Counterintelligence Awareness Training. As of July 2020, all EMCOR personnel had completed the training. Based on documentation provided to us by EMCOR, 42 percent of subcontractor personnel had completed the training ([redacted] subcontractor personnel) as of September 11, 2020.

Although FDIC Directive 1600.7 required EMCOR and its subcontractors to complete the Insider Threat and Counterintelligence Awareness Training, the Facilities Management Contract did not contain such a requirement, because the FDIC established Directive 1600.7 after the Facilities Management Contract was awarded. In addition, the Oversight Manager was not aware of the requirement in FDIC Directive 1600.7 for contractor and subcontractor personnel to complete this Insider Threat and Counterintelligence Awareness training.

Lack of Training Posed Risk to the FDIC

EMCOR and its subcontractor personnel have wide-ranging unescorted physical access to the Virginia Square facility, including its offices, cubicles, file rooms, and restricted areas. Many of these areas contain large amounts of sensitive hardcopy information, such as confidential bank examination information, including supervisory ratings; human resources information, including personally identifiable information; procurement sensitive information; and sensitive law enforcement data. Individuals who do not complete the Information Security and Privacy Awareness Training are less likely to be familiar with requirements for safeguarding such information. This lack of training (knowledge) increases the risk that these individuals will not comply with Federal security and privacy laws and policies, or recognize when and how to report potential violations. Completing required security training is also critical for

ensuring that personnel understand that they will be held accountable for non-compliance with FDIC security and privacy requirements.

Further, contractor and subcontractor personnel who do not complete the FDIC's Insider Threat and Counterintelligence Awareness Training may not be informed of potentially suspicious activity that could place FDIC personnel and facilities at risk, and therefore, they may not know how to identify and report insider threats.

Insider Threat and Counterintelligence Awareness Training is particularly important for personnel who have access to critical building infrastructure, such as fire and life safety systems; electrical and utility systems; air handling and distribution equipment; water systems; network IT systems and equipment; and emergency fuel tanks and generators. Such infrastructure can be attractive targets for insider threats intent on harming the FDIC and its personnel.

Recommendations

We recommend that the Deputy to the Chairman and Chief of Staff and COO:

7. Ensure that all contractor and subcontractor personnel on the Contract required to complete Information Security and Privacy Awareness Training and Insider Threat and Counterintelligence Awareness Training have done so.

8. Conduct training to ensure that all Oversight Managers understand the requirement for contractor and subcontractor personnel to complete Information Security and Privacy Awareness Training and Insider Threat and Counterintelligence Awareness Training.

9. Ensure that Oversight Managers assigned to other FDIC contracts have verified the completion of Information Security and Privacy Awareness Training and Insider Threat and Counterintelligence Awareness Training for contractor and subcontractor personnel without network access.

10. Include a provision in future contracts requiring contractor and subcontractor personnel to complete Insider Threat and Counterintelligence Awareness Training.

FDIC COMMENTS AND OIG EVALUATION

FDIC management provided a written response, dated March 16, 2021, to a draft of this report. The response is presented in its entirety in Appendix 5. In the response, management concurred with all 10 of the report's recommendations.

Following the issuance of the draft report, DOA provided us with documentation to support that it had taken corrective action to address 2 of the report's 10 recommendations. We reviewed the documentation provided by DOA and confirmed that it was responsive to the two recommendations. Accordingly, we closed both recommendations. The report's other eight recommendations will remain open until we confirm that the FDIC has completed corrective actions and the actions are responsive. Appendix 6 contains a summary of the FDIC's corrective actions.

We also provided EMCOR with a draft copy of the report to review for factual accuracy. We considered EMCOR's informal feedback before finalizing the report.

Objective

The objective of the audit was to assess whether the FDIC had implemented effective controls to protect electrical power; HVAC; and water services at its Virginia Square facility. The audit focused on the effectiveness of security controls over three systems used by the FDIC, EMCOR, and its subcontractors to monitor, manage, and ensure the uninterrupted delivery of critical building services—[redacted], and [redacted]. Consistent with NIST guidance,[42] we assessed the effectiveness of system security controls by determining the extent to which they were implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the systems. The audit also assessed whether the FDIC ensured compliance with key security provisions in the Facilities Management Contract.

We conducted this performance audit from October 2019 through January 2021 in accordance with generally accepted government auditing standards. Those 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.

Scope and Methodology

We assessed the effectiveness of internal controls that we deemed significant to the audit objective. Specifically, we assessed 10 of the 17 principles associated with the 5 components of internal control defined in the Government Accountability Office's *Standards for Internal Control in the Federal Government* (September 2014) (Green Book).[43] The Table below summarizes the principles we assessed.

Table: Internal Controls Assessed

Control Environment
Principle 2 Exercise oversight responsibility
Principle 3 Establish structure, responsibility, and authority
Principle 5 Enforce accountability
Risk Assessment
Principle 6 Define objectives and risk tolerances
Principle 7 Identify, analyze, and respond to risk
Control Activities

[42] See NIST SPs 800-53, Rev.4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013), and 800-53A, Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations* (December 2014).
[43] The Green Book organizes internal control through a hierarchical structure of 5 components and 17 principles. The 17 principles support the effective design, implementation, and operation of the components, and represent the requirements for establishing an effective internal control system.

Principle 11 Design activities for the information system
Principle 12 Implement control activities
Information and Communication
Principle 14 Communicate internally
Monitoring
Principle 16 Perform monitoring activities
Principle 17 Remediate deficiencies

Source: OIG analysis of the Green Book and work performed on this audit.

The report presents the internal control deficiencies we identified within the findings. Because our audit was limited to the principles presented in the Table, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit. The following section provides details regarding the procedures we performed to conduct our audit and assess internal controls relevant to the audit objective.

To address the audit objective, we:

- Reviewed the Facilities Management Contract and interviewed EMCOR, DOA, and OCISO personnel to obtain an understanding of the security controls and practices used by the FDIC to protect critical building services.

- Reviewed key Facilities Management Contract deliverables and FDIC reports, such as contractor status reports, inspection reports, preventative maintenance schedules, inventories of mechanical equipment, and reports of service calls.

- Assessed the extent to which the FDIC implemented the NIST RMF for [redacted], and [redacted].

- Examined reports and supporting documentation for all user accounts for [redacted], and [redacted] to determine whether: [redacted]

- Determined whether [redacted], and [redacted] were supported by current versions of the manufacturers' software.

- Determined whether EMCOR and its subcontractors complied with key terms and conditions of the Facilities Management Contract, including the completion of scheduled preventative maintenance over critical building assets; the tracking of critical equipment; the execution of confidentiality agreements; and the completion of FDIC-required training.

- Reviewed the After Action reports prepared by the FDIC for the 2014 Data Center power outage and the 2019 water interruption to obtain an understanding of the corrective actions the FDIC took (or planned to take).

We relied on computer processed information to conduct our analysis of user accounts and scheduled preventative maintenance of critical assets. We corroborated the computer processed information we used with information from other sources, such as direct examination, supporting documentation, and testimonial evidence from subject matter experts. We determined that the computer processed information we used in our analysis was sufficiently reliable for the purposes of our audit.

We also reviewed FDIC-generated risk management reports at both the enterprise and divisional level to determine the extent to which the FDIC was assessing risks associated with OT systems. These reports included the FDIC's Risk Inventory and Risk Profile. We also reviewed information in the FDIC's Enterprise Risk Management tool and DOA's annual Assurance Statement for 2019.

To assess compliance with laws and regulations, we evaluated the FDIC's implementation of relevant provisions of FISMA, OMB Circular A-130, NIST security standards and guidelines, and FDIC policies and procedures.

We used the following NIST security standards and guidelines as criteria:

- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004);
- SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations* (December 2018)*;*
- SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013)*;* and
- SP 800-82, Rev. 2, *Guide to Industrial Control Systems (ICS) Security* (May 2015).

We used the following FDIC policies as criteria:

- Directive 1360.9*, Protecting Sensitive Information* (April 2007)*;*
- Directive 1360.10, *Corporate Password Standards* (February 2003);
- Directive 1360.16, *Mandatory Information Security Awareness Training* (July 2002);
- Directive 1600.7*, FDIC Insider Threat and Counterintelligence Program* (September 2016)*;* and
- Directive 1610.2, *Personnel Security and Suitability Program for Contractors and Contractor Personnel* (January 2020).

We performed our work at the FDIC's Virginia Square offices in Arlington, Virginia, and at other off-site locations in the Washington, D.C., metropolitan area.

Appendix 2 Acronyms and Abbreviations

CEFile	Contract Electronic File
CIOO	Chief Information Officer Organization
CISO	Chief Information Security Officer
COO	Chief Operating Officer
DHS	Department of Homeland Security
DOA	Division of Administration
EMCOR	EMCOR Government Services, Inc.
FDIC	Federal Deposit Insurance Corporation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
Green Book	Standards for Internal Control in the Federal Government
HVAC	Heating, Ventilation, and Air Conditioning
IT	Information Technology
IoT	Internet of Things
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
OT	Operational Technology
[redacted]	[redacted]
RMF	Risk Management Framework
[redacted]	[redacted]
SP	Special Publication
[redacted]	[redacted]
Virginia Square Facility	FDIC's L. William Seidman Center

Office of Inspector General

Federal Deposit Insurance Corporation
Office of Inspector General
Office of Information Technology Audits and Cyber

Date: March 20, 2020

Memorandum To: Arleas Upton Kea
Deputy to the Chairman and Chief Operating Officer

Zachary N. Brown
Chief Information Security Officer

/Signed/

From: Mark F. Mulholland
Assistant Inspector General for Information Technology Audits and Cyber

Subject: **Management Advisory Memorandum** | Concerns Related to the Security of a Server Supporting the [redacted] System | Audit No. 2020-001

While conducting our ongoing audit of *Critical Building Services at FDIC-owned Buildings*, we identified concerns related to the security of a server[1] supporting the [redacted] system [redacted] [redacted] is a building automation system used in the Virginia Square facility to monitor critical services, such as electrical power; heating, ventilation, and air conditioning; water pressure; and fire alarm protection. Although we have not yet completed our review of the server, we are sharing our concerns so that you may take prompt action.

Background

In October 2014, the FDIC entered into a Consolidated Facilities Management Contract with EMCOR Government Services, Inc. (EMCOR). Under the contract, EMCOR and its subcontractors operate a number of building automation systems at FDIC-owned facilities in the Washington, D.C. area. One such system is [redacted].

[redacted] monitors the operation of critical mechanical equipment and services at the Virginia Square facility. For example, [redacted] monitors building water pressure, which is critical to the health and safety of building occupants and the proper operation of the systems that cool the FDIC's National Data Center. If [redacted] detects a change in water pressure that falls outside of normal parameters, [redacted] notifies EMCOR and FDIC personnel via a text message to their handheld devices.

On November 8, 2019, [redacted] detected a drop in water pressure at the Virginia Square facility. According to the Chief Information Officer Organization's (CIOO) Awareness Report

[1] According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, *Security Guide for Interconnecting Information Technology Systems* (August 2002), a server is a computer or device on a network that manages network resources. Examples include Web servers that store, process, and deliver Web pages, and database servers that store data and process queries.

(November 12, 2019), this event caused the cooling systems that provide air conditioning to National Data Center to lose efficiency, causing the temperature in the National Data Center to rise. The CIOO's Awareness report states that without adequate water, the cooling systems will eventually stop working, making the National Data Center too hot for the computer equipment to continue operating. In response, CIOO staff powered down some of its network information technology (IT) equipment in the National Data Center to reduce heat output, and transferred certain IT services to its back-up site. The FDIC also closed its offices in the Virginia Square facility.

Concerns

On March 4, 2020, we performed an initial review of an [redacted] server supporting the [redacted] system. This server is physically located in the Virginia Square facility. The audit team noted the following security concerns:

- **Obsolete** [redacted] NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013), recommends that organizations replace their information system components when support for those components is no longer available from the developer, vendor, or manufacturer. NIST SP 800-53, Rev. 4, [redacted]
- **Potentially Vulnerable IT Services.** We identified two IT services enabled [redacted]
  - [redacted]
  - [redacted]

[2] [redacted]

[redacted]

- **Security Audit Log Not Reviewed.** NIST SP 800-53, Rev. 4, recommends that organizations review and analyze information system audit logs for indications of inappropriate or unusual activity. According to NIST SP 800-92, *Guide to Computer Security Log Management* (September 2006), security audit logs contain a record of events[5] occurring within an organization's information systems and networks. The security audit log for the server contained [redacted] events. However, the FDIC had not reviewed the log for inappropriate or unusual activity, including cyberattacks. We brought the matter to the attention of the FDIC's Chief Information Security Officer, who stated that members of his staff would conduct a review of the security audit log.

- **Password Not Encrypted.** The server contained multiple files on its hard drive. The audit team observed a CIOO representative open one of these files and noted that the file contained a password in an unencrypted (plaintext) format.[6] NIST SP 800-53, Rev. 4, recommends that passwords be stored in an encrypted format. Storing passwords in plaintext increases the risk that the password will be compromised and used for malicious activity, such as disrupting the server's operation.

Conclusion

Because the server supporting [redacted] is [redacted], it can be subject to cyberattacks. Accordingly, the server should be properly secured and monitored.

We request that you provide us with a written response to this memorandum describing the actions the FDIC plans to take to address the concerns described above, along with the timeframes for completing those actions. Please submit your response by April 3, 2020.

If you have any questions or would like to discuss these concerns, please contact me at [redacted] or Joe Nelson, Audit Manager, [redacted].

cc: Daniel H. Bender, DOA
Brian Yellin, DOA
Stephen Beard, DOA
William J. Gately, DOA
Sylvia W. Burns, CIO
Montrice G. Yakimov, CIOO
E. Marshall Gentry, Division of Finance

[3] [redacted]
[4] [redacted]
[5] Events include such things as password changes, failed logins, administrative privilege usage, and third-party credential usage.
[6] Encryption is a process that changes plaintext information (data that can be read) into ciphertext (data in an encrypted format).

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

Chief Operating Officer
Office of the Chief Information Security Officer

DATE: April 6, 2020

MEMORANDUM TO: Mark F. Mulholland
Assistant Inspector General for
Information Technology Audits and Cyber

FROM: ARLEAS KEA Digitally signed by ARLEAS KEA Date: 2020.04.06 13:16:18 -04'00'
Arleas Upton Kea
Deputy to the Chairman and Chief Operating Officer

Zachary N. Brown
Chief Information Security Officer ZACHARY BROWN Digitally signed by ZACHARY BROWN Date: 2020.04.06 09:21:06 -04'00'

SUBJECT: Management Advisory Memorandum: Concerns Related to the Security of a Server Supporting the [redacted] System
Audit No. 2020-001

Thank you for the opportunity to provide a written response to the subject OIG management advisory memorandum. In its memorandum, the OIG identified concerns related to the security of a server supporting the [redacted] system ([redacted], a tool used by the FDIC's facilities management contractor (EMCOR) to monitor building services, including water pressure, electrical power distribution, emergency electrical backups, and HVAC. As you know, representatives of the Corporate Services Branch (CSB) and the Office of the Chief Information Security Officer (OCISO) took immediate steps to discuss and begin evaluating the issues and concur they warrant attention.

Our response provides information on the functionality provided by the [redacted] tool, responsibility for its maintenance, where it resides in the FDIC's information technology environment, and potential risks associated with exploitation of the security weaknesses identified by the OIG. We also describe the actions we have taken and planned to address those weaknesses.

We appreciate your staff's time and effort and we expect the actions taken in response to this advisory memorandum will increase the FDIC's assurance that our building systems are adequately secured and monitored and mitigate the reputational risk of someone exploiting the server for illicit activity.

Background Information on the [redacted] Tool

[redacted] is a commercially available product manufactured by [redacted] for entities needing a solution to monitor facilities mechanical equipment. [redacted] assists EMCOR engineers and FDIC staff with monitoring over 2,000 data points of building services. Under its contract with the FDIC, EMCOR is responsible for maintaining [redacted] including software patches, revisions and/or bug fixes to the current software that may be periodically created by the existing

manufacturer to maintain present system operations. In some cases, CSB has chosen not to proceed with upgrades based on the cost involved, as the FDIC is contractually responsible for paying any amount in excess above $7,500.

[redacted] sends a text message each morning and afternoon that provides a "heartbeat test" that notifies appropriate staff it is functioning properly. On the rare occasion the tool is not functioning properly, additional EMCOR engineers are put on duty to monitor critical systems.

[redacted] is maintained on a workstation and [redacted] that resides in a locked electrical room adjacent to the Virginia Square Data Center. Access to that room is restricted to certain FDIC facilities staff and EMCOR staff have access. The data [redacted] gathers is transmitted through a [redacted] provided by an [redacted] and completely separated from the FDIC network, which mitigates the risk of unauthorized access to FDIC systems and data. We concur, however, that there are the following risks:

- A [redacted] on this facility monitoring product could interrupt or alter data used to monitor building systems (to the extent facilities personnel are unable to monitor the systems manually);
- Interruption of updates and maintenance of the server; and
- If an adversary were able to use [redacted] as [redacted] the contractual relationship between the vendor and the FDIC could create a reputational risk to the FDIC.

Corrective Actions Taken and Planned

On March 26, 2020, CSB officials participated in a conference call with EMCOR and [redacted] to discuss the concerns raised in the advisory memorandum. [redacted] provided options that will be incorporated into a proposal that will be sent to EMCOR and the FDIC within the next several days. [redacted] will be able to install these options within thirty days from approval. Upon receipt of the proposal, CSB will consult with OCISO on how to proceed.

In addition, the Security Operations Section performed a review of the security logs on the Foreseer setup as recommended in the advisory memorandum. The review revealed that the vast majority of the security log events were [redacted]. This type of activity is typically associated with [redacted]. The logs revealed only [redacted] and no indication of a successful log-in or access by unauthorized users.

We also have [redacted] with similar, and even improved functionality, as part of a capital improvement project that includes implementing an upgraded [redacted] and [redacted] at Virginia Square. We expect this project to begin in the second quarter of 2021 and be completed approximately a year later.

If you have any questions regarding this response, please contact Jenna Mathieson at [redacted] or Brian Yellin at [redacted]

cc: Marshall Gentry
Isaac Hernandez
Sylvia Burns
Brian Yellin

3

On May 8, 2020, we issued an Advisory Memorandum to the CISO describing two potential security vulnerabilities identified during the audit. Neither of these vulnerabilities affect the building services within the scope of this report.

The first potential vulnerability related to the configuration of a public website supporting the [redacted]. The FDIC remediated this potential vulnerability during the course of our audit. The second potential vulnerability involved an [redacted] IT computing device with certain [redacted] that, if not properly configured, could be compromised.

In a written response to our Advisory Memorandum, dated May 22, 2020, the CIO and CISO stated that the IT computing device was an [redacted] used to monitor the [redacted]. The response stated that the FDIC used a vendor to maintain the [redacted], and that the device was not connected to the [redacted]. To address our concerns regarding the [redacted], the CIO and CIOO stated that the CIOO would work with DOA to:

- Share our observations about the [redacted] on the [redacted] with the vendor so they could be evaluated and secured or disabled to align with best practices; and

- Explore the feasibility of expanding the language in the FDIC's contract with the vendor that covers the maintenance of the [redacted].

On February 2, 2021, a representative of the CIOO provided the status of the FDIC's actions to address our concerns regarding the [redacted]. The CIOO representative stated that the CIOO and DOA had determined that modifying the configuration of the [redacted] on the [redacted] was not viable. DOA plans, instead, to develop new IT security requirements for the [redacted] that the FDIC intends to incorporate into a replacement contract. In addition, the OCISO will review these IT security requirements prior to contract award in order to ensure that they address potential risks associated with the [redacted] and facilities-related monitoring functions.

Office of Inspector General

Federal Deposit Insurance Corporation
Office of Inspector General
Office of Information Technology Audits and Cyber

Date: May 8, 2020

Memorandum To: Zachary N. Brown
Chief Information Security Officer

/Signed/

From: Mark F. Mulholland
Assistant Inspector General for Information Technology Audits and Cyber

Subject: **Management Advisory Memorandum** | Potential Security Vulnerabilities Related to the [redacted] Website and an IT Computing Device | No. 2020-001

The purpose of this memorandum is to notify you of two potential security vulnerabilities that came to our attention while conducting our ongoing audit of *Critical Building Services at FDIC-owned Buildings*. We notified a representative of the Office of the Chief Information Security Officer (OCISO) of these potential security vulnerabilities on April 29, 2020.

[redacted] Website

The FDIC maintains a public-facing website that any Internet user can access at [redacted][1] This website contains a search engine that allows users to search for information maintained by the [redacted].

As of April 29, 2020, this website, however, also contained [redacted]

IT Computing Device

In addition, we identified an information technology (IT) computing device [redacted] that was separate from the website described above.[2] As of April 29, 2020, this IT computing device appeared to have certain [redacted]

[1] The Internet Protocol (IP) Address for this website is [redacted].
[2] The IP Address for this IT device is [redacted] The IT device appeared to be an FDIC desktop or laptop computer.

[redacted]

[redacted] If not properly patched and configured, [redacted] could allow an attacker to gain unauthorized access to the IT device and perform malicious activity. [redacted] If not properly configured, a malicious actor could exploit vulnerabilities in the [redacted] to [redacted] and view sensitive information [redacted]

We request that you provide a written response to this Memorandum describing the actions the OCISO plans to take to address the potential security vulnerabilities described above. Please submit your response by May 22, 2020.

If you have any questions or would like to discuss the issues discussed in this memorandum, please contact me at [redacted] or Joe Nelson, Audit Manager, at [redacted].

cc: Arleas Upton Kea, Deputy to the Chairman and COO
Daniel H. Bender, DOA
Brian Yellin, DOA
Stephen Beard, DOA
William J. Gately, DOA
Sylvia W. Burns, CIO
Montrice G. Yakimov, CIOO
E. Marshall Gentry, DOF

[redacted]

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

DATE: May 22, 2020

TO: Mark F. Mulholland
Assistant Inspector General for
Information Technology Audits and Cyber

FROM: Sylvia W. Burns
Chief Information Officer and Chief Privacy Officer SYLVIA BURNS Digitally signed by SYLVIA BURNS Date: 2020.05.22 17:08:15 -04'00'

Zachary N. Brown
Chief Information Security Officer ZACHARY BROWN Digitally signed by ZACHARY BROWN Date: 2020.05.22 17:06:07 -04'00'

SUBJECT: Management Response to the Advisory Memorandum Entitled *Potential Security Vulnerabilities Related to the* [redacted] *Website and an IT Computing Device | No. 2020-001*

Thank you for the opportunity to provide a written response to the Office of Inspector General's (OIG) Advisory Memorandum on the *Potential Security Vulnerabilities Related to the* [redacted] *Website and an IT Computing Device*, issued May 8, 2020. In its memorandum, the OIG documented two concerns. The first concern dealt with an FDIC public facing website[1] that contained [redacted]. The second concern dealt with an IT computing device with [redacted]. We examined both of the concerns that the OIG raised, and the FDIC subsequently took remedial action to address the first concern.

Our response provides information on the functionality of the public website and the computing device, and describes the actions we have taken and planned to address the items identified in your advisory memorandum. We appreciate your staff's time and effort and we expect the actions taken and planned in response to this advisory memorandum will increase the FDIC's assurance that our [redacted] and building systems are adequately secured. Cybersecurity is critical to the FDIC's ability to carry out its mission of maintaining stability and public confidence in the nation's financial system and continues to be a top priority at the FDIC.

[1] [redacted]

MANAGEMENT RESPONSE

Advisory Area 1 – [redacted] Website

The OCISO coordinated with the FDIC's Chief of [redacted] in the Division of Administration (DOA), to address the items noted by the OIG. The FDIC utilizes the [redacted] website to provide FDIC personnel access to search the FDIC [redacted]

Although some of the available content on the [redacted] contained [redacted] to [redacted], those [redacted] were not actually accessible. The [redacted] were [redacted] non-functioning [redacted] " [redacted]" domain, formerly the FDIC's [redacted] domain. The FDIC retired the [redacted] domain in December 2018 as part of a technical upgrade to the FDIC [redacted]. The FDIC has removed the [redacted] In addition, the [redacted] is working with the vendor that maintains the site, [redacted] to evaluate the need for continued availability of the site from the Internet.

Advisory Area 2 – IT Computing Device

The IT Computing Device referenced in the advisory memorandum is an [redacted] device that is not [redacted] The [redacted] is a technology component of a contracted service to support " [redacted] also known as [redacted] This service is associated with the [redacted] According to the [redacted] website,[3] "this program allows [redacted] participation in the [redacted] is instrumental in determining the activation [redacted]

The contractor, [redacted] maintains the current [redacted] and an [redacted] maintenance program. The vendor's [redacted] device is not connected to the [redacted] and it does not process FDIC information. The use, configuration and operation of the device is managed by the contractor in support of the [redacted] program. The CIOO will work with DOA to relay the observations noted in the advisory memorandum to the vendor such that the protocols noted by the OIG can be evaluated and secured or disabled to align with best practices.

The OIG's analysis in the area of devices associated with monitoring FDIC facilities is appreciated. The CIOO will work with DOA to evaluate the contract with [redacted] and explore the feasibility of expanding existing language covering the maintenance of the vendor's device. More broadly, the FDIC will pursue a risk-based approach to identify, assess

[2] [redacted]

[3] [redacted]

and manage potential risks associated with devices or services performing facilities-related monitoring functions.

Any questions regarding this response should be directed to Zachary Brown, Chief Information Security Officer.

cc: Isaac Hernandez, Deputy Director, DIT, Infrastructure Services Branch
Montrice G. Yakimov, Chief, IT Governance, Risk, and Policy Section, OCMS

3

Federal Deposit Insurance Corporation

MEMO

TO: Mark F. Mulholland
Assistant Inspector General for Information Technology Audits and Cyber

FROM: Brandon L. Milhorn BRANDON MILHORN Digitally signed by BRANDON MILHORN Date: 2021.03.15 22:35:59 -04'00'
Deputy to the Chairman, Chief of Staff and Chief Operating Officer

Zachary N. Brown
Chief Information Security Officer Digitally signed by ZACHARY BROWN Date: 2021.03.15 22:08:29 -04'00'

CC: Sylvia W. Burns, CIO
E. Marshall Gentry, CRO

DATE: March 16, 2021

RE: Management Response to OIG Draft Audit Report, Security of Critical Building Services at FDIC-Owned Facilities (No. 2020-001)

The FDIC has completed its review of the Office of Inspector General's (OIG) draft audit report titled Security of Critical Building Services at FDIC-Owned Facilities dated February 12, 2021. In its report, the OIG identified a number of findings and recommendations related to security and internal controls for several systems we use to support the safe and reliable operation of critical building equipment and services.

The FDIC concurs with all ten of the OIG's recommendations. The FDIC is committed to addressing each of the recommendations within the designated timeframes.

As noted in the report, the FDIC took immediate steps to mitigate risks identified by the OIG in an advisory memorandum it issued during the fieldwork phase of its audit. Specifically, FDIC installed a firewall, updated [redacted] disabled vulnerable IT services, and conducted a forensic review and found no evidence of unauthorized access for one of the building systems reviewed. We also upgraded the software on a second building services system in response to the OIG's findings. As a result, we have substantially reduced the residual risk of operating the building systems addressed in this audit.

In addition to the corrective actions we describe below, the FDIC has taken steps to ensure building systems and services like those covered in this audit will have cost-effective controls commensurate with risk. Specifically, the FDIC has implemented a centralized demand management function that ensures IT needs are evaluated and dispositioned in a strategic manner, and that solutions are secure and consistent with the FDIC's architecture. Further, the FDIC now requires that program office Information Security Managers and the Office of the Chief Information Security Officer (OCISO) review contracts to ensure that appropriate security and privacy controls are incorporated into contract provisions. These steps support the FDIC's implementation of the National Institute of Standards and Technology (NIST) Risk Management Framework.

Federal Deposit Insurance Corporation

Finally, the FDIC has initiated planning and research efforts to replace certain building systems with an integrated facilities and workplace management solution with increased functionality and current technology and security.

Management Response to Recommendations

Recommendation 1: Include systems supporting critical building services in FDIC-owned facilities in the FDIC's systems inventory.

Management Decision: Concur

Corrective Action: OCISO will coordinate with the Corporate Services Branch (CSB) to identify systems supporting building services and their corresponding contract(s) and include them in FDIC's systems inventory.

Estimated Completion Date: June 30, 2021

Recommendation 2: Implement the NIST Risk Management Framework for systems supporting critical building services.

Management Decision: Concur

Corrective Action: OCISO will coordinate with CSB and the Legal Division to review contract language in contracts that support critical building services. The Acquisition Services Branch (ASB) will modify or renew such contract(s) to include requirements to implement the NIST Risk Management Framework as needed.

Estimated Completion Date: December 31, 2021

Recommendation 3: Modify the Facilities Management Contract to define security requirements for systems that support critical building services in FDIC-owned facilities.

Management Decision: Concur

Corrective Action: ASB will negotiate a modification to the current Facilities Management Contract that includes the appropriate security requirements for systems that support building services.

Estimated Completion Date: June 30, 2021

Recommendation 4: Obtain completed Confidentiality Agreements for all EMCOR and subcontractor personnel required to execute such agreements under the Facilities Management Contract, and maintain copies in the FDIC's contracting files.

Management Decision: Concur

Corrective Action: When advised of this finding during the audit, CSB obtained the Confidentiality Agreements (CAs) for all EMCOR and subcontractor personnel and placed them in CEFile.

Completion Date: Completed

MEMO 2

Federal Deposit Insurance Corporation

Recommendation 5: Ensure that Oversight Managers assigned to other FDIC contracts have obtained signed Confidentiality Agreements for all contractor and subcontractor personnel required to sign such agreements.

Management Decision: Concur

Corrective Actions: ASB will issue a communication to remind Oversight Managers (OMs) of the requirement to obtain signed CAs for contractor and subcontractor personnel. In addition, ASB will request that OMs review their active award files and provide confirmations they have obtained signed CAs from contractor and subcontractor personnel, as applicable. In addition, ORMIC will conduct compliance reviews of select active contracts, the scope of which will include determining whether required CAs have been collected and filed, and will report the results to Division/Office management.

Estimated Completion Dates:

- Communication to OMs: April 30, 2021
- OM confirmations that CAs have been obtained, as applicable: May 31, 2021
- Complete first series of compliance reviews: December 31, 2021

We note that the FDIC also requires that contractors complete a Confidentiality Agreement at the firm level as a condition of the engagement. The requirement that individual contractor and subcontractor personnel sign such agreements is an additional measure to ensure their awareness and facilitate holding them accountable for any violation, should that occur. The FDIC intends to perform a review to identify opportunities for strengthening our existing processes used to obtain and file the CAs. We will advise the OIG of the timing and results of that review once scheduled and complete.

Recommendation 6: Provide training to Oversight Managers to ensure that Confidentiality Agreements are consistently executed and maintained as required by FDIC policy.

Management Response: Concur

Corrective Action: ASB will develop focused CA training and make it available to Oversight Managers. The focused training will address Form 3700/46A, *Confidentiality Agreements for Contractor and Subcontractor Personnel*, and the Oversight Manager's responsibility to receive and upload signed CAs to CEFile.

Estimated Completion Dates:

- Develop focused CA training for OMs: May 31, 2021
- Deliver training for OMs assigned to active contracts: June 30, 2021

Recommendation 7: Ensure that all contractor and subcontractor personnel on the Contract required to complete Information Security and Privacy Awareness Training and Insider Threat and Counter Intelligence Awareness Training have done so.

Management Response: Concur

Corrective Action: CSB took corrective action to address this finding during the course of the audit. As a result,

MEMO 3

FDIC Federal Deposit Insurance Corporation

all contractor and subcontractor personnel assigned to the Contract have completed the required Information Security and Privacy Awareness Training and Insider Threat and Counter Intelligence Awareness Training.

Completion Date: Completed

Recommendation 8: Conduct training to ensure that all Oversight Managers understand the requirement for contractor and subcontractor personnel to complete Information Security and Privacy Awareness Training and Insider Threat and Counter Intelligence Awareness Training.

Management Response: Concur

Corrective Actions: ASB, in consultation with OCISO and CSB, will develop and make available focused training to OMs that provides guidance on when and how contractor and subcontractor personnel must complete both training courses and instructions for OMs on documenting training completion in CEFile.

Estimated Completion Dates:

- ASB develops focused training for OMs: May 31, 2021
- ASB delivers training for OMs assigned to active contracts: June 30, 2021

Recommendation 9: Ensure that Oversight Managers assigned to other FDIC contracts have verified the completion of Information Security and Privacy Awareness Training and Insider Threat and Counter Intelligence Awareness Training for contractor and subcontractor personnel without network access.

Management Response: Concur

In conjunction with the communication to Oversight Managers (OMs) on obtaining CAs for contractor and subcontractor personnel, ASB will request that OMs review their active award files and provide confirmations that contractor and subcontractor personnel without network access have completed Information Security and Privacy Awareness Training and Insider Threat and Counter Intelligence Awareness Training. In addition, ORMIC will include coverage of this training requirement in its compliance reviews of select active contracts.

- Communication to OMs: April 30, 2021
- OM confirmations that training has been completed, as applicable: May 31, 2021
- Complete first series of compliance reviews: December 31, 2021

Recommendation 10: Include a provision in future contracts requiring contractor and subcontractor personnel to complete Insider Threat and Counter Intelligence Awareness Training.

Management Response: Concur.

Corrective Action: ASB will issue a PAB and modify standard contract templates, as needed, to ensure that future contracts include contract provisions requiring contractor and subcontractor personnel to complete Insider Threat and Counter Intelligence Awareness Training.

Estimated Completion Date: June 30, 2021

MEMO 4

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

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	OCISO will coordinate with DOA's Corporate Services Branch (CSB) to identify systems supporting building services and their corresponding contract(s) and include them in the systems inventory.	June 30, 2021	$0	Yes	Open
2	OCISO will coordinate with CSB and the Legal Division to review contracts supporting building services. DOA's Acquisition Services Branch (ASB) will modify or renew such contract(s) to include requirements to implement the NIST Risk Management Framework as needed.	December 31, 2021	$0	Yes	Open
3	ASB will negotiate a modification to the Facilities Management Contract that includes appropriate security requirements for systems supporting building services.	June 30, 2021	$0	Yes	Open
4	CSB obtained completed Confidentiality Agreements for all EMCOR and subcontractor personnel required to execute such agreements and placed them in CEFile.	March 9, 2021	$0	Yes	Closed
5	ASB will remind Oversight Managers of the requirement to obtain Confidentiality Agreements for contractor and subcontractor personnel. In addition, Oversight Managers will review their active award files to confirm they have obtained required Confidentiality Agreements. Further, the Office of Risk Management and Internal Controls (ORMIC) will conduct compliance reviews of select active contracts, the scope of which will include determining whether required Confidentiality Agreements have been collected and filed. ORMIC will report the results of its reviews to Division and Office management.	December 31, 2021	$0	Yes	Open

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
6	ASB will develop and deliver training on Confidentiality Agreements for Oversight Managers. The training will cover Oversight Manager responsibilities for receiving and uploading completed Confidentiality Agreements into the CEFile.	June 30, 2021	$0	Yes	Open
7	All contractor and subcontractor personnel assigned to the Facilities Management Contract completed Information Security and Privacy Awareness Training and Insider Threat and Counterintelligence Awareness Training.	March 9, 2021	$0	Yes	Closed
8	ASB will develop and deliver training to Oversight Managers on when and how contractor and subcontractor personnel must complete Information Security and Privacy Awareness Training and Insider Threat and Counterintelligence Awareness Training, as well as how completed training will be documented.	June 30, 2021	$0	Yes	Open
9	ASB will request that Oversight Managers review their active award files and confirm that contractor and subcontractor personnel without network access have completed Information Security and Privacy Awareness Training and Insider Threat and Counterintelligence Awareness Training. In addition, ORMIC will cover this training requirement in its compliance reviews of select contracts.	December 31, 2021	$0	Yes	Open
10	ASB will issue a Procurement Administrative Bulletin and modify the FDIC's standard contract templates, as needed, to ensure that future contracts include provisions requiring contractor and subcontractor personnel to complete Insider Threat and Counterintelligence Awareness Training.	June 30, 2021	$0	Yes	Open

[a] Recommendations are resolved when —

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

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

Federal Deposit Insurance Corporation
Office of Inspector General

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

(703) 562-2035

★★★★★★

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

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