Review of the FDIC's Ransomware Readiness

March 2024 **REV-24-01**

Review Report

Audits, Evaluations, and Cyber

☆☆☆☆☆☆☆☆

REDACTED VERSION
PUBLICLY AVAILABLE
The redactions contained in this report are based upon requests from FDIC senior management to protect the Agency's information from disclosure.

NOTICE

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

Office of Inspector General

Executive Summary

Review of the FDIC's Ransomware Readiness

According to the Cybersecurity & Infrastructure Security Agency (CISA), ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and systems that rely on them unusable. The number and impact of publicly reported ransomware incidents has made ransomware a significant risk in today's cybersecurity landscape. The goal of most ransomware incidents is to halt processes, interrupt services, and cause disruption until a ransom payment is made in exchange for decrypting files and systems. Ransomware can severely impact business processes and leave organizations without the data they need to operate or deliver mission-critical services. The organizations affected often experience reputational damage, significant remediation costs, and interruptions in their ability to deliver core services.

The Federal Deposit Insurance Corporation (FDIC) relies heavily on information systems to carry out its responsibilities of insuring deposits; examining and supervising financial institutions for safety, soundness, and consumer protection; making large and complex financial institutions resolvable; and managing receiverships. Therefore, it is important for the FDIC to have effective controls for safeguarding its information systems and data to reduce the risk that a ransomware incident could disrupt critical operations and allow inappropriate access to, and disclosure, modification, or destruction of, that FDIC information.

The objective of this review was to assess the adequacy of the FDIC's process to respond to a ransomware incident.

Results

Overall, we determined that the FDIC had an adequate process to respond to a ransomware incident and generally followed applicable guidance and best practices within the five control areas that we assessed.[1] Specifically, the FDIC developed and communicated applicable incident response and ransomware-specific policies and plans that include roles and responsibilities for personnel in various FDIC Divisions in a disaster recovery event, such as a ransomware incident. The FDIC

[1] We assessed the following five control areas: Ransomware Policy, Ransomware Playbook, Backup and Recovery, Crisis Communication, and Staffing and Third-Party Support. See Table 1 in Appendix 1 for a description of each control area.

also developed and maintained a Continuity Implementation Plan, which established the organization, actions, and procedures necessary to recover critical Information Technology (IT) functions in case of a business disruption.

Further, the FDIC created and maintained multiple iterations of backup data for Mission Essential (ME)/Mission Critical (MC) systems,[2] to facilitate data recovery in the event of a ransomware incident. Finally, the FDIC established a contract for cybersecurity incident detection and response services to provide containment and remediation support in the event of a ransomware incident.[3]

With that said, we noted the FDIC did not fully adhere to Federal standards, FDIC policies, and/or industry best practices in the following areas:

1. Protecting backup data and testing the capability to restore systems from backups.
2. Maintaining a current, complete, and accurate Continuity Implementation Plan.
3. Enabling Wireless Priority Service access for all FDIC Chief Information Officer Organization Executive Management Emergency Command Team (CEMECT) Members.
4. Ensuring that key individuals completed Disaster Recovery Awareness Training.

As a result, weaknesses in some controls and practices could affect the ability of the FDIC to respond to a ransomware incident, including:

1. the inability to prevent ransomware incidents from impacting its backup data;
2. the inability to restore and recover all critical information technology services from backups consistent with Agency established objectives;
3. challenges for key disaster response or recovery personnel to communicate during an incident; and

[2] "Mission Essential" is defined as a system whose loss would cause a stoppage of the core operations supporting the FDIC's mission. "Mission Critical" refers to a system whose loss would produce a significant impact on the FDIC's operations, but not its core mission.

[3] The contract for cybersecurity incident detection and response services includes threat intelligence, security analytics, monitoring, investigation, and incident response. Specific services include: on-call remote support for incident monitoring and response; on-site support for incident monitoring and response activities at FDIC facilities and FDIC controlled financial institutions, as needed; and utilization of cybersecurity tools and technology to support analysis, containment, and remediation of incidents, including a ransomware incident if it occurred.

4. challenges for individuals in the disaster recovery process to understand their roles and responsibilities.

Recommendations

We are making eight recommendations to strengthen the FDIC's process to respond to a ransomware incident. Specifically, we recommend that the FDIC evaluate and implement solutions to protect backup data; evaluate and consider enhanced solutions to store backup data; review and update policies and procedures to ensure timely control implementation of new Federal requirements; test recovery of Active Directory from backups; ensure the Continuity Implementation Plan is regularly updated in a timely manner to ensure it is current, complete, and accurate; periodically review and update key personnel enrolled in Wireless Priority Service and perform quarterly testing as part of its Emergency Communications Program; and ensure that key individuals complete Disaster Recovery Awareness Training.

The FDIC concurred with all of our recommendations. The FDIC plans to complete all corrective actions by February 28, 2025.

Contents

Office of Inspector General

Federal Deposit Insurance Corporation
Office of Inspector General
Audits, Evaluations, and Cyber

March 20, 2024

Subject | ***Review of the FDIC's Ransomware Readiness***

According to the Federal Deposit Insurance Corporation (FDIC), the number and impact of publicly reported ransomware incidents has made ransomware a significant risk in today's cybersecurity landscape.[4] Over the past year, there continued to be a significant number of high-profile ransomware incidents against corporations, state and local government entities, and non-profits. Further, according to the Government Accountability Office (GAO), the Department of Homeland Security has reported that ransomware is a serious and growing threat to government operations at the Federal, state, and local levels.[5] On a broader level, ransomware continues to pose a significant threat to U.S. critical infrastructure sectors, including finance and banking, as the number of attacks continues to increase.[6] The organizations affected often experience reputational damage, significant remediation costs, and interruptions in their ability to deliver core services.

According to the Cybersecurity & Infrastructure Security Agency (CISA), ransomware is an ever-evolving form of malware designed to encrypt files on a device,[7] rendering any files and systems that rely on them unusable. The goal of most ransomware incidents is to halt processes, interrupt services, and cause disruption until a ransom payment is made in exchange for decrypting files and systems and restoring access. Ransomware can severely impact business processes and leave organizations without the data they need to operate or deliver mission-critical services.

The FDIC relies heavily on information systems to carry out its responsibilities of insuring deposits; examining and supervising financial institutions for safety, soundness, and consumer protection; making large and complex financial institutions resolvable; and managing receiverships. Without effective controls for safeguarding its information systems and data, the FDIC would be at increased risk of a ransomware incident that could disrupt critical operations and allow inappropriate access to, and disclosure, modification, or destruction of, that FDIC information.

The objective of this review was to assess the adequacy of the FDIC's process to respond to a ransomware incident. Ransomware prevention and detection

[4] FDIC, *2023 Report on Cybersecurity and Resilience* (June 2023).
[5] GAO, *Ransomware: Federal Agencies Provide Useful Assistance but Can Improve Collaboration*, GAO-22-104767 (September 2022).
[6] FDIC, *Risk Review 2023.*
[7] Examples of devices include network storage, cloud storage, external hard drive storage, USB thumb drives, laptops, and smartphones.

measures were not in the scope of this review. Similarly, this review was not a comprehensive review of data governance or incident response. Appendix 1 contains information about the objective, scope, methodology, and control areas tested.

BACKGROUND

Ransomware Threats to Government Organizations

Ransomware poses threats to Federal, state, and local government organizations. According to CISA, the Federal Government must improve its efforts to protect against malicious cyber campaigns to ensure the security of Federal information technology (IT) assets.[8] In 2023, the GAO continued to recognize *Ensuring the Cybersecurity of the Nation* as a high risk across the Federal Government and stated that risks to technology systems are increasing. In particular, malicious actors are becoming more willing and increasingly capable of carrying out cyberattacks that could result in serious harm to human safety, the environment, and the economy.[9]

Similarly, the Council of the Inspectors General on Integrity and Efficiency (CIGIE) listed *Cybersecurity* as a key area of concern and cited evolving cyber threats, such as the growth in availability and effectiveness of internet-based hacking tools and recent threats from foreign adversaries to gain unauthorized access to sensitive data, slow or halt Government operations, access intellectual property and research, or gather useful intelligence.[10]

According to the GAO, cybercrimes in the U.S. have resulted in hundreds of billions of dollars in losses, and threaten public safety and economic security. The victims are widespread and include individuals, schools, businesses, utilities, and governments. For example, ransomware attacks—an increasingly common and dangerous form of cybercrime—have been launched against public elementary and secondary schools across the country. During these attacks, schools' computer systems were hijacked using malicious software, preventing their use and resulting in monetary losses to individual school districts of up to $1 million, as well as weeks of lost learning. In another example, the U.S. Marshals Service reported in February 2023, that it had been the victim of a ransomware attack where hackers accessed sensitive files, including information about investigative targets and employees' personal data.[11]

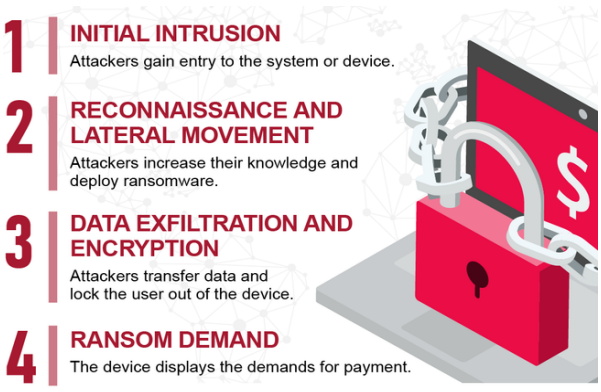
[8] CISA, *Binding Operational Directive 22-01-Reducing the Significant Risk of Known Exploited Vulnerabilities* (November 3, 2021).
[9] *GAO, High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (April 2023).
[10] CIGIE, *Top Management and Performance Challenges Facing Multiple Federal Agencies* (September 2023).
[11] GAO, *The U.S. Is Less Prepared to Fight Cybercrime Than It Could Be* (August 2023).

Ransomware Risks to the FDIC

According to the Multi-State Information Sharing & Analysis Center (MS-ISAC),[12] malicious actors have adjusted their ransomware tactics to be more destructive and impactful and have also exfiltrated[13] victims' data and pressured victims to pay by threatening to release the stolen data.[14] These ransomware and associated data breach incidents can severely affect business processes by leaving organizations unable to access necessary data to operate and deliver mission-critical services.

A ransomware attack often has a series of events that starts with an attacker gaining entry to the system or device by exploiting weak internal controls. **Figure 1** illustrates the four stages of a ransomware attack, according to the GAO.

Figure 1: Four Stages of a Ransomware Attack



Source: GAO, *Ransomware: Federal Coordination and Assistance Challenges* (November 2022).

The FDIC relies heavily on information systems, data, and personnel to carry out its mission. The FDIC is custodian of about 1.8 petabytes of sensitive and Personally Identifiable Information relating to failed banks and more than 4,700 insured banks. FDIC systems also contain sensitive information, such as Social Security Numbers and bank account numbers for FDIC employees and depositors of failed financial institutions; confidential bank examination information, including supervisory ratings; and sensitive financial data, including credit card numbers.

Recognizing the risk of a ransomware incident to the FDIC, in 2020, the FDIC's Office of Risk Management & Internal Controls (ORMIC) performed a limited review to better understand (1) the risks the FDIC faces from a potential ransomware incident, (2) government and commercial recommendations for mitigating the risks and negative outcomes associated with ransomware incidents, and (3) the information security controls the FDIC has put in place to address the possibility of a ransomware incident.

[12] The mission of the MS-ISAC is to improve the overall cybersecurity posture of the U.S., State, Local, Tribal, and Territorial government organizations through coordination, collaboration, cooperation, and increased communication.
[13] Exfiltration is the unauthorized transfer of information from an information system.
[14] MS-ISAC, *#StopRansomware Guide* (May 2023).

ORMIC concluded that the FDIC was well positioned to protect against a ransomware or other data integrity incident, detect such an incident if it occurs, and respond successfully by restoring the compromised information assets from secured backups. Additionally, ORMIC made suggestions to further strengthen the FDIC's ransomware response processes.[15]

Roles and Responsibilities

The FDIC has designated key individuals across the organization who are trained and ready to collaboratively respond to a ransomware incident. These stakeholders have roles and responsibilities that would prepare a response to a ransomware incident, ranging from remediating the ransomware incident itself, to assisting in communicating with the Chairman, the media, and the Congress if needed.

Chief Information Officer Organization (CIOO)

The CIOO has responsibility for IT governance, investments, program management, as well as cybersecurity and privacy. Within the CIOO, the Chief Information Security Officer is responsible for the Agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the FDIC. Also within the CIOO, the Division of Information Technology (DIT) conducts the day-to-day IT operations of the FDIC.

CIOO Executive Management Emergency Command Team (CEMECT)

The CEMECT is the governing body for all IT recovery efforts, and in the event of a business disruption, such as a ransomware incident, the activation of the CIOO Emergency Management Center occurs for the monitoring of recovery operations. In the event of an emergency, the CEMECT serves as the single point of contact for communicating across the FDIC to recover information technology services.

Division of Administration (DOA)

The DOA has overall responsibility for acquisition, corporate, and human resource services for the FDIC. The Crisis Readiness and Response Section within DOA is responsible for providing communication services (Emergency Notification Services and Wireless Priority Service (WPS)[16]) to communicate with internal and external parties during a cyber-event, such as a ransomware incident. The Crisis Readiness and Response Section also maintains enterprise-wide responsibility for the development and publication of response plans as well as management of the FDIC's emergency communications program.

[15] FDIC, *Limited Review of FDIC's Ransomware Preparedness* (February 2020).
[16] WPS is a White House-directed cellular communications service provided and managed by CISA in compliance with Federal Communications Commission. WPS provides authorized devices with priority calling on all nationwide and several regional cellular networks. WPS calls do not preempt calls in progress or deny the general public's use of the telephone network. WPS carriers activate eligible devices which enables priority calling on the service providers' networks when the *272 service code is dialed. Calls made with WPS overcome network congestion/degradation and complete with a success rate of 95 percent.

Office of Communications (OCOM)

OCOM is responsible for providing timely information about the FDIC's policies and programs to the media, the public, the financial services industry, and FDIC employees. In the event of a breach, OCOM is responsible for developing and executing a Corporate-wide breach communications plan for breaches as directed by the Chairman or designee. OCOM helps draft and approve external notification and communications; responds to breach-related inquiries or complaints; and initiates and organizes any press releases about the breach, if required.

Office of Legislative Affairs (OLA)

The OLA serves as the FDIC's Congressional liaison in the event applicable Congressional committees and members of Congress need to be notified. The OLA is also responsible for responding to requests from various Congressional committees, members, or their staff about the incident or breach.

Controls Assessed During Our Review

To assess the adequacy of the FDIC's process to respond to a ransomware incident, we reviewed the following five control areas covered by applicable guidance and best practices: Ransomware Policy, Ransomware Playbook, Backup and Recovery, Crisis Communication, and Staffing and Third-Party Support. **Table 1** in Appendix 1 contains descriptions for the control areas we tested.

REVIEW RESULTS

Overall, we determined that the FDIC had an adequate process to respond to a ransomware incident and generally followed applicable guidance and best practices within the five control areas that we assessed.[17] Specifically, the FDIC developed and communicated applicable incident response and ransomware-specific policies and plans to personnel in various FDIC Divisions that would have a role in a disaster recovery event, such as a ransomware incident. These policies and plans addressed areas recommended by the National Institute of Standards and Technology (NIST) and CISA, such as: roles and responsibilities; detection, recovery, and post-incident activities; processes, procedures, and workflows; and communication requirements and specific steps for appropriate stakeholders.

The FDIC also developed and maintained a Continuity Implementation Plan, which established the organization, actions, and procedures necessary to recover critical Information Technology (IT) functions in case of a business disruption. The

[17] See Table 1 below for the control areas.

Continuity Implementation Plan included necessary information, such as: locations where business data are processed, stored, transmitted or accessed; recovery time objectives; [18] and prioritization of data restoration efforts. In addition, the FDIC created and maintained multiple iterations of backup data for Mission Essential (ME)/Mission Critical (MC) systems, to facilitate data recovery in the event of a ransomware incident.

Further, the FDIC developed and conducted customized Disaster Recovery Awareness Training based on audience background and positions. Based on a sample of attendees, we concluded that the objectives of these training sessions were met and shared feedback collected from those attendees with appropriate Agency personnel for their consideration. The FDIC also conducted annual tabletop exercises with individuals that would have a role in a disaster recovery event, such as a ransomware incident. These were discussion-based exercises where participants met to validate the content of policies and plans by discussing their roles during an event and their responses to a particular event situation.

Finally, the FDIC established a contract for cybersecurity incident detection and response services to provide containment and remediation support in the event of a ransomware incident. The contract includes threat intelligence, security analytics, monitoring, investigation, and incident response. Specific services include: on-call remote support for incident monitoring and response; on-site support for incident monitoring and response activities at FDIC facilities and FDIC controlled financial institutions, as needed; and utilization of cybersecurity tools and technology to support analysis, containment, and remediation of incidents, including a ransomware incident if it occurred.

With that said, the FDIC did not fully adhere to Federal standards, FDIC policies, and/or industry best practices in the following areas:

1. Protecting backup data and testing the capability to restore systems from backups.
2. Maintaining a current, complete, and accurate Continuity Implementation Plan.
3. Enabling WPS access for all FDIC Chief Information Officer Organization Executive Management Emergency Command Team (CEMECT) Members.
4. Ensuring that key individuals completed Disaster Recovery Awareness Training.

[18] The Recovery Time Objective defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on supported mission/business processes. The faster system resources are successfully restored, the less time the mission/business is impacted.

As a result, weaknesses in some controls and practices could affect the ability of the FDIC to respond to a ransomware incident, including:

1. the inability to prevent ransomware incidents from impacting its backup data;
2. the inability to restore and recover all critical information technology services from backups consistent with Agency established objectives;
3. challenges for key disaster response or recovery personnel to communicate during an incident; and
4. challenges for individuals in the disaster recovery process to understand their roles and responsibilities.

Finding #1: The FDIC Did Not Effectively Protect Backup Data and Test the Capability to Restore Systems from Backups

The FDIC did not effectively protect backup data from (b) (7)(E) and test the capability to restore two ME/MC systems from backups.

(b) (7)(E) According to FDIC officials, since the backup data center used to be located in Manassas, VA, about 25 miles away from VASQ, this created a geographic proximity risk. The FDIC established a backup data center in another region of the country to mitigate this risk, which FDIC officials believed made (b) (7)(E)

According to the MS-ISAC, it is important to maintain (b) (7)(E), "as many ransomware variants[21] attempt to (b) (7)(E) to make restoration impossible unless the ransom is paid."[22] Similarly, the Federal Bureau of Investigation (FBI) recently warned of new data destruction tactics in ransomware incidents

(b) (7)(E)

[21] A variant refers to a new version of malware based on existing ransomware with modifications.
[22] MS-ISAC, *#StopRansomware Guide*, (May 2023).

and recommended that organizations maintain (b) (7)(E) of data, and regularly maintain backup and restoration.[23]

(b) (7)(E)
The FDIC is not using available solutions to ensure its backup data are
(b) (7)(E)

According to NIST SP 800-53 Revision 5, organizations should implement cryptographic protection to system backup information at both primary and alternate locations to prevent unauthorized disclosure and modification.[26] According to the Office of Management and Budget (OMB), agencies are expected to meet the requirements of, and be in compliance with, new or updated material in NIST standards and guidelines within one year of their respective publication dates unless otherwise directed by OMB.[27]

In response to our concern, the FDIC directed us to its *NIST SP 800-53 Revision 5 Baseline Control Requirements* document,[28] initially released in January 2022, which included the new cryptographic protection requirement for system backup information. However, an FDIC official responsible for implementing the new cryptographic protection requirements informed the Office of Inspector General (OIG) in August 2023, they were operating under the guidance of NIST SP 800-53 Revision 4, which did not extend the cryptographic protection requirement to system backup information. While CIOO officials provided documentation to support they had a policy in place to identify, assess, track and report on new Federal IT requirements and had communicated NIST SP 800-53 Revision 5 requirements with relevant stakeholders, they did not provide a specific cause for the untimely implementation of the new cryptographic protection control. Further, the FDIC's Storage

[23] FBI, *Two or More Ransomware Variants Impacting the Same Victims and Data Destruction Trends*, (September 2023).
(b) (7)(E)
(b) (7)(E)
[26] NIST Special Publication (SP) 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, (September 2020).
[27] OMB Circular A-130, *Managing Information as a Strategic Resource*, (July 2016).
[28] This document provides program offices, information owners and others with helpful guidance and specifications to assist in planning and implementing security and privacy controls. These controls are derived from Federal requirements and standards.

Systems Backup Data Protection Standard Operating Procedures[29] did not include instructions to encrypt its backup data for the primary and backup data centers.

(b) (7)(E) [redacted]

Testing Active Directory Restoration From Backups

The FDIC did not test its ability to restore Active Directory[31] from a backup during its annual disaster recovery exercises, even though the FDIC produces backups. Specifically, instead of restoring Active Directory from a backup during the FDIC's annual disaster recovery exercises, the FDIC cut the connection to one domain controller[32] and tested whether applications could connect to the other domain controllers. In response to the OIG's concerns, CIOO officials stated it was not necessary or beneficial to test a full restoration of the Active Directory backup data. Specifically, they stated that the FDIC has about 26 Active Directory domain controllers across the United States and believe these redundancies eliminated the necessity to ever restore Active Directory from a backup copy because, in the event that one domain controller fails, the other domain controllers will automatically provide comparable functionality.

In addition, CIOO officials stated it would be very difficult to test fully restoring Active Directory from a backup and would be disruptive since many processes rely on Active Directory. Further, CIOO officials stated a full recovery from a backup would affect the Recovery Time Objective and the Recovery Point Objective.[33] However, the CIOO's statements do not consider an attack that might compromise Active Directory and we believe there may be viable alternatives, yet to be explored, for testing restoration of Active Directory.[34] These alternatives may provide assurance that the FDIC would be able to successfully and fully restore

[29] This Standard Operating Procedure covers implementation and maintenance of procedures for the backup of FDIC data and an aspect of data protection: system backups for the purpose of recovering data in case of equipment failure, fire, flood, catastrophe, user error or any other event.

(b) (7)(E) [redacted]

[31] Active Directory is a commonly used directory service developed by the Microsoft Corporation that controls system access across an Agency's network.

[32] A domain controller is a server that runs Active Directory and responds to authentication requests on a network.

[33] The Recovery Point Objective represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. The more recent the successful backup copy, the less data that may be potentially lost due to an outage.

[34] Such alternatives may include restoring Active Directory from a backup in an isolated environment.

from backups in the event of a ransomware incident in line with MS-ISAC guidance and best practices.

Impacts of Not Testing Restoration from Backups. According to the MS-ISAC, organizations should regularly test the availability and integrity of backups in a disaster recovery scenario. Ransomware attackers often search for backups of targeted data. According to the FBI, in early 2022, multiple ransomware groups increased use of custom data theft, wiper tools, and malware to pressure victims to negotiate.[35] In other words, these groups used tools to steal or erase the victims' data. Without (b) (7)(E), the FDIC increases its risk of ransomware incidents compromising ME/MC system backup data connected to its network. Additionally, without ensuring backup data is (b) (7)(E), the FDIC decreases its ability to prevent ransomware incidents from encrypting, corrupting, or deleting critical data stored in accessible backups, increasing the risk of not being able to recover that data.

Further, without periodic testing of the Active Directory backups, the FDIC cannot ensure it would be able to successfully and fully restore Active Directory from backups in the event of a ransomware incident. If the Active Directory database is corrupted or deleted, the FDIC may lose its Active Directory data and be unable to authenticate users or access resources stored in Active Directory. Finally, the FDIC may experience a disruption in services that rely on Active Directory, including email, file sharing, and network printing.

Recommendations

We recommend that the CIOO:

1. Evaluate and implement solutions to protect backup data, as described in the report, and update the Storage Systems Backup Data Protection Standard Operating Procedures, as appropriate.
2. Evaluate and consider enhanced solutions to store backup data, as described in the report, and update the Storage Systems Backup Data Protection Standard Operating Procedures, as appropriate.
3. Review and update policies and procedures for identifying, assessing, and tracking new Federal IT requirements to ensure timely control implementation, as appropriate.
4. Conduct an analysis to identify viable alternatives for testing restoration of Active Directory from backups, or have senior management formally accept the risk of not testing these backups.

[35] FBI, *Two or More Ransomware Variants Impacting the Same Victims and Data Destruction Trends*, (September 2023).

Finding #2: Current, Complete, and Accurate Continuity Implementation Plan Not Maintained

The FDIC did not maintain a current, complete, and accurate Continuity Implementation Plan (CIP). Specifically, we identified issues related to the (1) inventory of ME and MC systems; (2) policy of vital records; and (3) point of contact information.

The CIOO/DIT CIP identifies continuity requirements and procedures necessary to resume and continue information technology services for each Division and Office's essential and supporting business functions during an event, such as a ransomware incident. The CIP includes all the continuity of operations and disaster recovery contingency plans for DIT, which include (1) high-level plans (e.g., Business Continuity Plan (BCP)[36] and Emergency Response Plan[37]), (2) technical system/platform recovery plans, and (3) tools (e.g., Call Trees, Contact Lists, & Logistical Information).

Mission Essential/Mission Critical Systems Inventory

The FDIC did not maintain an updated BCP with all ME/MC systems and current system description information. We compared an inventory of ME/MC systems from the FDIC's Business Continuity and Disaster Recovery SharePoint site as of May 10, 2023, to the inventory from version 17 of the BCP (dated July 2021 and distributed on August 13, 2021). Based on our review, we identified two ME/MC systems that were included in the SharePoint site but missing from the BCP.[38] Additionally, an FDIC ME/MC system was renamed and was updated in the SharePoint site, but not in the BCP.[39]

According to the GAO, management should use quality information to make informed decisions and evaluate the entity's performance in achieving key objectives and addressing risks. Quality information is defined as appropriate, current, complete, accurate, accessible, and provided on a timely basis.[40]

[36] The Business Continuity Plan defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business disruption.
[37] The Emergency Response Plan provides guidance and direction in case of a disruption of service.
(b) (7)(E)
[redacted]
[40] GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (September 2014).

In addition, NIST states that an up-to-date Information System Contingency Plan[41] (ISCP) is essential to successful ISCP operations. As a general rule, the ISCP should be reviewed for accuracy and completeness at least annually, as well as upon significant changes to any element of the ISCP, system, mission/business processes supported by the system, or resources used for recovery procedures.[42]

During our review, the FDIC provided an updated version of the BCP (version 18, dated September 2023 and distributed on September 27, 2023), which included changes to the ME/MC list. We found that version 18 of the BCP now contained the three systems we identified as missing or not updated above.

Policy for Vital Records

We also found that the version 17 of the BCP contained outdated information regarding backup media. Specifically, the BCP contained Section 7 titled, *Vital Records*, that included references to backup tapes being stored offsite at Iron Mountain.

Additionally, we noted references to backup tapes and vital records as part of its assumptions for Scenario 1 (Section 6.1) and Scenario 2 (Section 6.2) in the BCP, which lists modes of transportation available for delivery of backup tapes and vital records to the recovery site. However, the FDIC does not (b) (7)(E) ME and MC system (b) (7)(E) . As previously discussed in Finding 1, in 2019, the FDIC discontinued (b) (7)(E)

During our review of the updated version 18 of the BCP, dated September 2023, we found that the FDIC removed the *Vital Records* section and replaced it with *Business Resumption*. Additionally, the BCP no longer contained references to backup tapes.

Point of Contact Information Discrepancies

Additionally, we found that version 17 of the BCP contained discrepancies regarding the telephone numbers listed for the Chief Information Officer (CIO)/DIT Director and CIO Acquisition Strategy & Innovation Branch (CASIB) Deputy Director.[43] Subsequently, during our review of version 18 of the BCP, dated September 2023, we found that the FDIC updated contact information for these individuals.

[41] According to NIST SP 800-34 Revision 1, an Information System Contingency Plan, such as the FDIC's Continuity Implementation Plan, provides established procedures for the assessment and recovery of a system following a system disruption.
[42] NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems (May 2010).
[43] The CIO/DIT Director serves as chairperson of the CEMECT and the CASIB Deputy Director is a member of the CEMECT.

According to the BCP, plan maintenance and distribution includes, but is not limited to, the continued endorsement of the plan through the review of the plan in no less than on an annual basis. Further, once published, the BCP would undergo continuous reviews and updates as procedures are changed; systems are installed, modified, or eliminated; or as the data center environment is changed, such as equipment replacement, upgrades, or removal; software upgrades or elimination, and reconfiguration of the data center.[44]

The FDIC did not have an effective process to update the CIP on a timely basis to ensure it is current, complete, and accurate. While CIOO officials referred to the CIP and its sub-sections as "living documents," they also stated it is only distributed and reviewed on a biennial basis (once every two years), or when there are major changes to the environment or organization. During our review, the FDIC distributed version 18 of the BCP on September 27, 2023 and we verified the discrepancies described above were updated.

Finally, CIOO officials did not believe that the BCP needed to be updated every time the BC/DR (Disaster Recovery) SharePoint was updated because the changes were not deemed significant enough to justify an update to the BCP. Further, version 17 of the CIP was the first version that was electronic, not hardcopy. Prior to version 17, the FDIC maintained only hardcopy versions of the CIP,[45] which the CIOO official stated were labor intensive to update and distribute, since any updates would necessitate printing multiple new hardcopies and hand delivering them to the appropriate recipients.

Without a current, complete, and accurate CIP, the FDIC may not be able to contact personnel critical to the disaster recovery process and ensure that they would sustain and recover all critical IT services following an emergency within the required Recovery Time Objectives. For example, if a ransomware incident had occurred during the time the BCP's ME and MC inventory was not up-to-date, the FDIC may not have been aware it needed to recover the three systems that were not accurately listed in the BCP's inventory, or the FDIC may not have correctly prioritized the restoration of these systems. These three systems contained the following critical information:

[44] FDIC, *Business Continuity Plan*, Version 17, (July 2021).
[45] The last hardcopy version of the CIP was distributed in 2018.

- (b) (7)(E) [redacted]
- (b) (7)(E) [redacted]
- (b) (7)(E) [redacted]

Recommendation

We recommend that the CIOO:

5. Develop a process to ensure the Continuity Implementation Plan is regularly updated in a timely manner to ensure it is current, complete, and accurate.

Finding #3: Wireless Priority Service Access Not Enabled for All CEMECT Members

The FDIC did not enable Wireless Priority Service (WPS) access for all CEMECT members. Although CIOO senior management officials believed that all CEMECT members had WPS enabled and CEMECT members attended a June 2, 2023, training where they were informed they should be enrolled in WPS, not all members had been enrolled by DOA.

Specifically, we found that as of June 2, 2023, based on documentation provided by the FDIC, six of the ten (60 percent) CEMECT members were not enrolled in WPS. In response, DOA activated WPS for these remaining six members. Also, the FDIC did not establish processes for CEMECT members to test WPS calling on a quarterly basis, as recommend by CISA. Specifically, CISA recommends that users make test WPS calls on a quarterly basis to ensure familiarity with making priority telecommunications calls.[46] CISA also states that calls made with WPS overcome network congestion/degradation; are completed with a 95 percent success rate and can connect to cellular, landline, and satellite phones.[47]

[46] CISA, *Making A Wireless Priority Service (WPS) Call* (May 2017).
[47] CISA, *Making A Wireless Priority Service (WPS) Call* (May 2017).

According to the GAO, management should obtain relevant[48] data from reliable[49] internal and external sources in a timely manner and evaluate both internal and external sources of data for reliability.[50] In addition, as stated previously, management should use quality information to make informed decisions and evaluate the entity's performance in achieving key objectives and addressing risks.

On June 26, 2023, DOA provided the OIG a listing showing only two CEMECT members with WPS activated. Finally, after DOA provided the OIG additional listings showing that CEMECT members had been incrementally added by DOA, on August 23, 2023, DOA provided an updated listing showing all ten CEMECT members having WPS active.

During our fieldwork, when asked about the discrepancy between these listings, the FDIC officials stated "there was an effort to reconcile access and provide access to those who needed it." In addition, since CEMECT members did not test WPS calling on a quarterly basis, some members were not aware their WPS access was not activated on their FDIC mobile device.

Without an accurate and complete listing of personnel with WPS access, the FDIC could experience challenges communicating with key disaster response or recovery personnel during a ransomware incident. For example, a ransomware incident may affect Microsoft Outlook, Teams, or any other Agency applications used for messaging and communication. WPS could be used in this instance by disaster recovery personnel who prioritize communication with other key recovery personnel.

Recommendation

We recommend that the Director, Division of Administration:

6. Develop and implement a process to periodically review and update key personnel enrolled in WPS, including those in the CIOO Executive Management Emergency Command Team, and perform quarterly testing as part of its Emergency Communications Program.

[48] Relevant data have a logical connection with, or bearing upon, the identified information requirements.
[49] Reliable internal and external sources provide data that are reasonably free from error and bias and faithfully represent what they purport to represent.
[50] GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (September 2014).

Finding #4: Key Individuals Did Not Complete Disaster Recovery Awareness Training

Initial DR Awareness Training

The FDIC did not ensure that new employees and contractors assigned a CIP role and individuals who changed positions or were assigned a new CIP role completed the DR Awareness Training within 30 days, as required by FDIC policy. Specifically, between January 1, 2023 and April 30, 2023, 26 of 33 new employees/contractors (79 percent) with a CIP role did not complete the required DR Awareness Training. In addition, as of June 2023, 76 of 80 employees (95 percent) that had transitioned to a CIP role/position did not complete the required DR Awareness Training.

The DR Awareness Training describes the FDIC's policies, procedures, plans, and the roles and responsibilities needed to successfully recover critical business functions during an emergency or disaster situation, including a ransomware incident. This training is important to help ensure that individuals understand their own roles and responsibilities and the roles and responsibilities of the other individuals and teams involved in the disaster recovery process so that the FDIC can successfully recover its critical business functions.

According to NIST, organizations should provide comprehensive role-based training to personnel with specific roles and responsibilities that addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls.[51] Further, FDIC Directive 1360.13 requires that Disaster Recovery Contingency Awareness Training is completed by all CIOO employees and contractor personnel identified as team members in the CIP within 30 days of assuming a contingency role.[52]

However, the FDIC did not have an effective process to ensure that employees and contractors in a CIP role were assigned initial and annual DR Awareness Training in the FDIC Learning Experience (FLX) system. For example, some individuals did not have an FLX account to complete the required training. In addition, the process to update the FLX system is a manual process with the Infrastructure Management Services Unit, which is responsible for DR Awareness Training, and Corporate University personnel using a shared spreadsheet.

As of October 18, 2023, the FDIC CIOO responded that the Infrastructure Management Services Unit had established a process to ensure that employees and contractors with a CIP role are assigned and complete the initial and annual Disaster Recovery Awareness Training in the FDIC's FLX system. In addition, the CIOO stated that as of October 19, 2023, Corporate University provided the FDIC Disaster

[51] NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020).
[52] FDIC Directive 1360.13, *Information Technology Continuity Implementation Program* (June 30, 2021).

Recovery team access to the FLX system, which allows them to add/or remove users that require training as needed.

Annual DR Awareness Training

The FDIC was unable to provide documentation that CIOO employees and contractor personnel identified as team members in the CIP completed DR Awareness Training annually, as required, because the FDIC did not track the date when individuals switched to a CIP role that required the DR Awareness Training. As stated previously, organizations should provide comprehensive role-based training to personnel with specific roles and responsibilities.

FDIC Directive 1360.13 requires that DR Awareness Training be completed by all CIOO employees and contractor personnel identified as team members in the CIP annually after completing initial training.[53] However, the FDIC did not monitor individuals' completion of the required annual DR Awareness Training.

All FDIC employees and contractor personnel identified as CIP team members need to understand their roles and responsibilities in the event of an incident or disaster as well as the roles and responsibilities of their fellow team members. For example, should a ransomware incident occur that affects the FDIC's data, the identified CIP team members need to know how and with whom to communicate, what steps to take to recover the affected data, and how they need to assess the damage caused by the ransomware incident.

If individuals in the disaster recovery process do not have an understanding of their roles and responsibilities, there is an increased risk that the FDIC's disaster recovery process may be adversely affected. These negative effects could include exposed and/or compromised data that would affect the FDIC's operations, mission, and reputation.

Recommendations

We recommend that the CIOO:

7. Develop and implement a process to ensure employees and contractors in a Continuity Implementation Plan role are assigned and complete initial Disaster Recovery Awareness Training in the FDIC Learning Experience system.
8. Develop and implement a process to ensure employees and contractors in a Continuity Implementation Plan role are assigned and complete annual Disaster Recovery Awareness Training in the FDIC Learning Experience system.

[53] FDIC Directive 1360.13, *Information Technology Continuity Implementation Program* (June 30, 2021).

FDIC COMMENTS AND OIG EVALUATION

On March 8, 2024, the CIOO and DOA provided a written response to a draft of this report. The response is presented in its entirety in Appendix 3.

In its response, the FDIC agreed with the findings and concurred with all eight report recommendations. The FDIC stated it had completed corrective actions for recommendations 1 and 6, and plans to complete corrective actions for the remaining six recommendations by February 28, 2025. We consider all eight recommendations to be resolved.

We reviewed the corrective actions for recommendations 1 and 6 and concluded they are closed. The other six recommendations will remain open until we confirm that corrective actions have been completed and the actions are responsive. A summary of the FDIC's corrective actions is contained in Appendix 4.

Appendix 1 Objectives, Scope, and Methodology

Objective

The objective of this review was to assess the adequacy of the FDIC's process to respond to a ransomware incident.

We conducted this review from March 2023 through January 2024. This review was performed in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Federal Offices of Inspector General*. These quality standards, as contained in the Pandemic Response Accountability Committee Agile Products Toolkit, include independence, analysis, evidence review, indexing and referencing, legal review, and supervision.

Scope and Methodology

The scope of this review focused on the adequacy of the FDIC's process to respond to a ransomware incident. Ransomware prevention and detection measures were not in the scope of this review. Similarly, this review was not a comprehensive review of data governance or incident response. Specifically, we assessed:

- The adequacy of the FDIC's Ransomware Policy and Playbook to determine whether the FDIC has plans in place to respond to and recover from a ransomware incident.
- The adequacy of the FDIC's Backup and Recovery Policy to determine whether the FDIC has taken steps to maintain encrypted backups of mission critical systems to timely recover from a ransomware incident.
- The FDIC's Crisis Communication Plan to determine whether the FDIC has plans in place for communicating with key stakeholders during a ransomware incident.
- The FDIC's staffing/support skillsets to determine whether FDIC employees and contractors have the knowledge and experience to respond effectively to a ransomware incident.
- The FDIC's third-party support requirements to determine whether the FDIC has established any capability to quickly bring in third-party support to respond to a ransomware incident.

To achieve our objective, we conducted the following procedures:

- Interviewed and surveyed FDIC officials and personnel in the following Divisions and Offices regarding FDIC policies and processes:
  - Division of Administration

  - Division of Information Technology
  - Legal Division
  - Chief Information Officer Organization
  - Corporate University
  - Office of the Chief Information Security Officer
  - Office of Communications
  - Office of Legislative Affairs
- Collected and reviewed survey responses from a judgmentally selected sample of system/data/business owners to confirm their involvement in identifying specific data to be backed up and in specifying at what frequency.
- Reviewed the results from annual disaster recovery exercises for 2020 – 2022.
- Attended the FDIC's annual privacy tabletop exercise. The simulation involved a departing FDIC employee who intentionally distributed documents containing Personally Identifiable Information for 100,000+ individuals. Attendees that participated were the following Agency officials or their designee: CIO, Chief Information Security Officer, Senior Agency Official for Privacy, Chief Operating Officer, Chief of Staff, Incident Response Coordinator, Privacy Section Chief, Director of OLA, General Counsel, Director of OCOM, Deputy to the Chairman for External Affairs, and the Security Operations Section Chief.
- Reviewed the FDIC's retainer contract for cybersecurity incident detection response services including threat intelligence, security analytics, monitoring, investigation, and incident response and security operations activities to determine what services would be available to the FDIC if a ransomware incident occurred.
- Reviewed applicable Federal regulations, Executive Orders, and standards for cybersecurity and internal controls:
  - NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020)
  - NIST SP 800-53 Revision 4, *Security and Privacy Controls for Information Systems and Organizations* (April 2013)
  - NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems* (May 2010)
  - NIST Interagency or Internal Report (NISTIR) 8374, *Ransomware Risk Management: A Cybersecurity Framework Profile* (February 2022)
  - NIST SP 800-184, *Guide for Cybersecurity Event Recovery* (December 2016)
  - OMB Circular A-130, Managing Information as a Strategic Resource (July 2016)
  - OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (January 2017)
  - GAO-14-704G, *Standards for Internal Control in the Federal Government* (September 2014)

- CISA, *Binding Operational Directive 22-01-Reducing the Significant Risk of Known Exploited Vulnerabilities* (November 2021)
- 12 C.F.R. Parts 309, 310

- Reviewed FDIC policies and procedures for cybersecurity and internal controls:
  - FDIC Directive 1360.13, *Information Technology Continuity Implementation Program* (June 2021)
  - FDIC Directive 4010.3, *Enterprise Risk Management and Internal Control Program* (October 2018)
  - FDIC, *Continuity Implementation Plan* Version 17 (July 2021)
  - FDIC, *Continuity Implementation Plan* Version 18 (September 2023)
  - FDIC, *Business Continuity Plan* Version 17 (July 2021)
  - FDIC, *Business Continuity Plan* Version 18 (September 2023)
  - FDIC, *Emergency Response Plan* Version 17 (July 2021)
  - FDIC, *Emergency Response Plan* Version 18 (September 2023)
  - FDIC, *Incident Response Plan* (2019)
  - FDIC Directive 1360.1, *FDIC Automated Information System (AIS) Security Program* (September 2003)
  - FDIC Directive 1360.15, *Access Control for Information Technology Resources* (January 2023)
  - FDIC Directive 1360.9, *Protecting Information* (July 2023)
  - FDIC Directive 1360.12, *Reporting Information Security Incidents* (August 2023)
  - *FDIC Security and Privacy Controls Assessment (SCA) Methodology* (March 2023)
- Reviewed applicable best practices (MS-ISAC, FBI, and others) for ransomware readiness and incident response including:
  - MS-ISAC, *#StopRansomware Guide* (May 2023)
  - FBI, *Two or More Ransomware Variants Impacting the Same Victims and Data Destruction Trends* (September 2023)
  - United States Computer Emergency Readiness Team (US-CERT), *Data Backup Options* (2012)
  - CISA, *Making A Wireless Priority Service (WPS) Call* (May 2017)
  - NIST, *Recovering from a Cybersecurity Incident: What to do Before and After* (December 2017)
- Reviewed reports from GAO, CIGIE, and other OIGs that have performed work related to cybersecurity and ransomware readiness including:
  - GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas* (GAO-23-106203) (April 2023)
  - CIGIE, *Top Management and Performance Challenges Facing Multiple Federal Agencies* (September 2023)

  - Department of Homeland Security OIG Report, *DHS Can Better Mitigate the Risks Associated with Malware, Ransomware, and Phishing Attacks* (OIG-22-62) (August 2022)
  - AmeriCorps OIG Report, *AmeriCorps' Penetration Testing and Phishing Campaign* (OIG-EV-22-06) (July 2022)
  - Tennessee Valley Authority OIG Report, *TVA's Internet Perimeter* (2020-15723) (November 2021)
  - Treasury Inspector General for Tax Administration Report, *The Endpoint Detection and Response Solution Has Been Deployed to Most Workstations and Is Operating As Intended, but Improvements Are Needed* (2021-20-065) (September 2021)

- Assessed the adequacy of the FDIC's process to respond to a ransomware incident in five control areas covered by applicable guidance and best practices. See **Table 1** below for the control areas.

Table 1: Description of Assessed Controls

Control Area	Description
Ransomware Policy	▪ Identify the person or department responsible for communicating the ransomware policy. ▪ Ensure that individuals charged with handling ransomware events have offline access to the ransomware playbook. ▪ Ensure that awareness sessions are customized based on audience background and positions. ▪ Obtain documentation that session frequency, content, and required attendees align with the ransomware policy. ▪ Determine if the identified awareness training session objectives were met.
Ransomware Playbook	▪ Verify that the FDIC has an approved ransomware playbook that addresses: o roles and responsibilities; o detection, recovery, and post-incident activities; o processes, procedures and workflows; o communication requirements and specific steps for appropriate stakeholders; and o negotiation and ransom payment policy(ies). ▪ Compare the FDIC's Ransomware Playbook to NIST guidance. ▪ Compare the FDIC's Ransomware Playbook to Federal guidance and best business practices. ▪ Compare the FDIC's Ransomware Playbook to NIST and CISA checklists. ▪ Compare the FDIC's Ransomware Playbook to Microsoft best practices.
Backup and Recovery	▪ Obtain FDIC backup and recovery policy(ies). Confirm that the policy(ies) include(s): o locations where business data are processed, stored, transmitted or accessed; o recovery point objectives; o recovery time objectives; and o prioritization of data restoration efforts. ▪ Interview a judgmental sample of system/data/business owners and ensure appropriate metrics are captured/reported and that business owners are involved in validating that recovered data. ▪ Determine if the FDIC uses a backup system that lets multiple iterations be saved. ▪ Determine if FDIC maintains offline backups, tests backups and restoration, and ensures backup data is encrypted.

Crisis Communication	▪ FDIC crisis communication policy contents. ▪ Crisis communication policy formally supported to ensure effectiveness and efficiency. ▪ Ransomware -tailored internal and external announcements. ▪ Regulatory announcements. ▪ Engagement with law enforcement. ▪ Treasury resources to assist with negotiation.
Staffing and Third-Party Support	▪ Digital Forensics Capabilities. ▪ Use of digital forensics provider. ▪ Appropriate level of external support services. ▪ Plan to contact each service provider. ▪ Reporting requirements.

Source: OIG scope for this review.

Appendix 2

Acronyms and Abbreviations

BCP	Business Continuity Plan
CASIB	CIO Acquisition Strategy & Innovation Branch
(b) (7)(E)	[redacted]
CEMECT	CIOO Executive Management Emergency Command Team
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CIOO	Chief Information Officer Organization
CIP	Continuity Implementation Plan
CISA	Cybersecurity & Infrastructure Security Agency
DARE	Data At Rest Encryption
DIT	Division of Information Technology
DOA	Division of Administration
DR	Disaster Recovery
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FLX	FDIC Learning Experience
(b) (7)(E)	[redacted]
GAO	Government Accountability Office
(b) (7)(E)	[redacted]
ISCP	Information System Contingency Plan
IT	Information Technology
MC	Mission Critical
ME	Mission Essential
MS-ISAC	Multi-State Information Sharing & Analysis Center
NIST	National Institute of Standards and Technology
OCOM	Office of Communications
OIG	Office of Inspector General
OLA	Office of Legislative Affairs
OMB	Office of Management and Budget
ORMIC	Office of Risk Management & Internal Controls
WPS	Wireless Priority Service

FDIC Federal Deposit Insurance Corporation

MEMO

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

FROM: Sylvia W. Burns SYLVIA BURNS
Chief Information Officer, Chief Privacy Officer, and Director, Division of Information Technology
Daniel H. Bendler DANIEL BENDLER Digitally signed by DANIEL BENDLER Date: 2024.03.08 14:11:05 -05'00'
Deputy to the Chairman and Chief Operating Officer

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

DATE: March 8, 2024

RE: Draft Office of Inspector General Report, Entitled *Review of the FDIC's Ransomware Readiness* (No. 2023-004)

Thank you for the opportunity to review and comment on the subject draft report. The Office of Inspector General (OIG) issued the draft report on February 21, 2024. The objective of the OIG's review was to assess the adequacy of the FDIC's process to respond to a ransomware incident. The FDIC places a high priority on implementing effective controls and processes for responding to cyber threats, including ransomware incidents.

We are pleased that, overall, the OIG determined the FDIC had an adequate process to respond to a ransomware incident, and that the FDIC generally followed applicable guidance and best practices in the control areas assessed during the review. As detailed in the draft report, the OIG found that the FDIC:

- Developed and communicated applicable incident response and ransomware-specific policies and plans that included roles and responsibilities for personnel in a disaster recovery event, such as a ransomware incident;
- Developed and maintained a Continuity Implementation Plan that established the organization, actions, and procedures necessary to recover critical Information Technology (IT) functions in case of a business disruption;
- Created and maintained multiple iterations of backup data for the FDIC's Mission Essential/Mission Critical systems to facilitate data recovery in the event of a ransomware incident;
- Developed and conducted customized Disaster Recovery awareness training for staff, and performed tabletop exercises for individuals who would have a role in a disaster recovery event, such as a ransomware incident; and
- Established a contract for cybersecurity incident detection and response services to provide containment and remediation support in the event of a ransomware incident.

Notwithstanding these results, the OIG's review also found that the FDIC did not fully adhere to all relevant Federal standards, FDIC policies, and/or industry best practices. Specifically, the FDIC needed to: protect its

1

FDIC Federal Deposit Insurance Corporation

backup data and test the ability to restore systems from backups; maintain a current, complete, and accurate Continuity Implementation Plan; enable Wireless Priority Service access for all employees who need it; and ensure all relevant individuals complete Disaster Recovery Awareness training.

The draft report contains eight recommendations. Seven of the recommendations are addressed to the Chief Information Officer Organization (CIOO) of which one is completed. The remaining recommendation is addressed to the Division of Administration (DOA), which was also completed. FDIC management concurs with all eight recommendations. A summary of management's planned and completed corrective actions follows.

Recommendation 1 -

We recommend that the CIOO:

Evaluate and implement solutions to protect backup data, as described in the report, and update the Storage Systems Backup Data Protection Standard Operating Procedures, as appropriate.

Management Decision: Concur

Corrective Action: The CIOO implemented actions on August 22, 2023 to protect backup data as described in the OIG's draft report. In addition, the CIOO updated the Storage Systems Backup Data Protection Standard Operating Procedures and provided evidence of its implementation to the OIG on December 6, 2023.

Estimated Completion Date: Completed

Recommendation 2 -

We recommend that the CIOO:

Evaluate and consider enhanced solutions to store backup data, as described in the report, and update the Storage Systems Backup Data Protection Standard Operating Procedures, as appropriate.

Management Decision: Concur

Corrective Action: The CIOO will evaluate solutions to store backup data, as described in the report, and update the Storage Systems Backup Data Protection Standard Operating Procedures, as appropriate.

Estimated Completion Date: February 28, 2025

Recommendation 3 –

We recommend that the CIOO:

Review and update policies and procedures for identifying, assessing, and tracking new Federal IT requirements to ensure timely control implementation, as appropriate.

Management Decision: Concur

Corrective Action: The CIOO will review and update policies and procedures for identifying, assessing, and tracking new Federal IT requirements to ensure timely control implementation, as appropriate.

FDIC Federal Deposit Insurance Corporation

Estimated Completion Date: June 28, 2024

Recommendation 4 –

We recommend that the CIOO:

Conduct an analysis to identify viable alternatives for testing restoration of Active Directory from backups, or have senior management formally accept the risk of not testing these backups.

Management Decision: Concur

Corrective Action: The CIOO will assess alternatives for testing the restoration of the Active Directory from backups. If the CIOO does not identify a viable alternative solution, senior CIOO management will formally accept the risk.

Estimated Completion Date: October 31, 2024

Recommendation 5 –

We recommend that the CIOO:

Develop a process to ensure the Continuity Implementation Plan is regularly updated in a timely manner to ensure it is current, complete, and accurate.

Management Decision: Concur

Corrective Action: The CIOO will develop a process to update the Continuity Implementation Plan in a timely manner to ensure it remains current, accurate and complete.

Estimated Completion Date: August 30, 2024

Recommendation 6 –

We recommend that the Director, Division of Administration:

Develop and implement a process to periodically review and update key personnel enrolled in Wireless Priority Service (WPS), including those in the CIOO Executive Management Emergency Command Team, and perform quarterly testing as part of its Emergency Communications Program.

Management Decision: Concur

Corrective Action Completed: On May 17, 2023, DOA's Crisis Readiness and Response team requested that all FDIC Divisions, Offices, and Regions provide a list of personnel within their organizations who require both Government Emergency Telecommunications Service (GETS) and WPS capabilities. DOA subsequently updated the roster of personnel who need these capabilities based on the input received and established a quarterly testing schedule. The first test was conducted during the week of October 30, 2023, and a second test was conducted during the week of January 22, 2024. The next test is scheduled to occur during the week of April 22, 2024. DOA will re-validate and update the personnel roster on an annually basis; the next update is scheduled to occur in May 2024. The personnel roster and exercise records document management's implementation of this recommendation.

Estimated Completion Date: Completed

Recommendation 7 –

We recommend that the CIOO:

Develop and implement a process to ensure employees and contractors in a Continuity Implementation Plan role are assigned and complete initial Disaster Recovery Awareness Training in the FDIC Learning Experience system.

Management Decision: Concur

Corrective Action: The CIOO will finish ongoing work to develop and implement a process that ensures employees and contractors in a Continuity Implementation Plan role are assigned and complete initial Disaster Recovery Awareness Training in the FDIC Learning Experience system.

Estimated Completion Date: August 30, 2024

Recommendation 8 –

We recommend that the CIOO:

Develop and implement a process to ensure employees and contractors in a Continuity Implementation Plan role are assigned and complete annual Disaster Recovery Awareness training in the FDIC Learning Experience system.

Management Decision: Concur

Corrective Action: The CIOO will finish ongoing work to develop and implement a process to ensure employees and contractors in a Continuity Implementation Plan role are assigned and complete annual Disaster Recovery Awareness training in the FDIC Learning Experience system.

Estimated Completion Date: August 30, 2024

Appendix 4 Summary of the FDIC's Corrective Actions

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

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	The CIOO implemented actions on August 22, 2023 to protect backup data as described in the OIG's draft report. In addition, the CIOO updated the Storage Systems Backup Data Protection Standard Operating Procedures and provided evidence of its implementation to the OIG on December 6, 2023.	December 6, 2023	$0	Yes	Closed
2	The CIOO will evaluate solutions to store backup data, as described in the report, and update the Storage Systems Backup Data Protection Standard Operating Procedures, as appropriate.	February 28, 2025	$0	Yes	Open
3	The CIOO will review and update policies and procedures for identifying, assessing, and tracking new Federal IT requirements to ensure timely control implementation, as appropriate.	June 28, 2024	$0	Yes	Open
4	The CIOO will assess alternatives for testing the restoration of the Active Directory from backups. If the CIOO does not identify a viable alternative solution, senior CIOO management plans to formally accept the risk.	October 31, 2024	$0	Yes	Open
5	The CIOO will develop a process to update the Continuity Implementation Plan to ensure it remains current, accurate and complete.	August 30, 2024	$0	Yes	Open

Summary of the FDIC's Corrective Actions

6	On May 17, 2023, DOA's Crisis Readiness and Response team requested that all FDIC Divisions, Offices, and Regions provide a list of personnel within their organizations who require both Government Emergency Telecommunications Service (GETS) and WPS capabilities. DOA updated the roster of personnel who need these capabilities and established a quarterly testing schedule. The first test was conducted in October 2023, and a second test was conducted in January 2024. The next test is scheduled to occur in April 2024. DOA will re-validate and update the personnel roster annually; the next update is scheduled to occur in May 2024.	January 22, 2024	$0	Yes	Closed
7	The CIOO will finish ongoing work to develop and implement a process that ensures employees and contractors in a Continuity Implementation Plan role are assigned and complete initial Disaster Recovery Awareness Training in FLX.	August 30, 2024	$0	Yes	Open
8	The CIOO will finish ongoing work to develop and implement a process to ensure employees and contractors in a Continuity Implementation Plan role are assigned and complete annual Disaster Recovery Awareness Training in FLX.	August 30, 2024	$0	Yes	Open

[a] Recommendations are resolved when —

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

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

Federal Deposit Insurance Corporation
Office of Inspector General

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

(703) 562-2035

★★★★★★

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

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