Security Controls Over the FDIC's Wireless Networks

December 2022 **REV-23-001**

Review
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.

Office of Inspector General

Executive Summary

Security Controls Over the FDIC's Wireless Networks

The term, Wi-Fi, refers to wireless technology that allows internet enabled devices (laptops, tablets, and smartphones) to connect to wireless access points and communicate through a wireless network. Wi-Fi technology offers benefits to organizations, such as ease of deployment and installation and expanded network accessibility. However, Wi-Fi technology also presents security risks to the confidentiality, availability, and integrity of Federal Deposit Insurance Corporation (FDIC) data and its systems, because it is not bound by wires or walls and if not properly configured, is susceptible to signal interception and attack.

The FDIC collects and retains significant amounts of sensitive banking information and information on FDIC personnel, including Personally Identifiable Information (PII). Therefore, the FDIC must protect its systems and data through effective security controls. In 2019, the FDIC replaced its legacy Wi-Fi infrastructure to provide expanded Wi-Fi services with approximately 1,200 wireless access points. These access points provide enhanced functionality by allowing users to connect to Wi-Fi throughout the FDIC's buildings, but also increase security risks.

The objective of this review was to determine whether the FDIC has implemented effective security controls to protect its wireless networks.[1] The FDIC Office of Inspector General (OIG) engaged the professional services firm of TWM Associates, Inc. to conduct the technical aspects of this review.

Results

We found that the FDIC did not comply or partially complied with several practices recommended by the National Institute of Standards and Technology and Federal and FDIC guidance in the following five areas:

1. **Configuration of Wireless Networks:** The FDIC did not properly configure its Policy Manager, which enforces security policies for wireless network connectivity. Also, the FDIC's Chief Information Officer Organization's

[1] We performed this review in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Federal Offices of Inspector General (Silver Book). These quality standards, as contained in the Pandemic Response Accountability Committee Agile Products Toolkit (https://www.pandemicoversight.gov/media/file/agile-products-toolkit.pdf), include independence, analysis, evidence review, indexing and referencing, legal review, and supervision.

(CIOO) Wi-Fi Operations Group did not have control or awareness of the set-up and configuration of numerous wireless devices operating in FDIC buildings and facilities.

2. **Wireless Signal Strength:** The FDIC did not have processes to examine and modify the signal strength of wireless devices/networks broadcasting throughout its buildings and leaking outside of FDIC facilities.
3. **Security Assessments and Authorizations:** The FDIC did not maintain a current Authorization to Operate (ATO) for its wireless network and did not conduct sufficient continuous monitoring testing activities to support the Agency's ongoing authorization of its wireless network.
4. **Vulnerability Scanning:** The FDIC did not include certain wireless infrastructure devices in its vulnerability scans. In addition, the FDIC did not use credentialed scans on wireless infrastructure devices.
5. **Wireless Policies, Procedures, and Guidance:** The FDIC did not maintain policies and procedures addressing key elements of the FDIC's wireless networks, including roles and responsibilities for the CIOO's Wi-Fi Operations Group; procedures for remediating wireless equipment alerts; standards for configuration settings; updates of wireless inventory records; and detection of rogue access points.

As a result, the FDIC faces potential security risks based upon its current wireless practices and controls, including unauthorized access to the FDIC networks and insecure wireless devices broadcasting Wi-Fi signals. We determined that the FDIC had effective controls related to physical access controls of wireless devices, access control and encryption,[2] monitoring of user internet destinations on its wireless networks, and disabling legacy wireless networks.

Recommendations

This report contains eight recommendations intended to strengthen the security controls over the FDIC's wireless networks. Specifically, we recommend that the FDIC: (1) ensure that wireless security weaknesses are tracked and remediated; (2) review, approve, and centrally manage the configuration settings of all FDIC Wi-Fi enabled devices; (3) identify wireless devices that should not be broadcasting inside and leaking outside buildings and take appropriate measures; (4) regularly examine wireless devices and broadcast areas to determine appropriate mitigation measures; (5) develop and provide training on the use of vendor hardening guidelines; (6) ensure all wireless devices are included in vulnerability scans;

[2] Access control is the process of granting or denying specific requests to obtain and use information and related information processing services. Encryption is the process of converting information or data into an unreadable format to prevent unauthorized access.

(7) enhance the vulnerability scanning process for the wireless infrastructure; and (8) ensure policies, procedures, and standards reflect current business practices and key aspects of wireless data communications.

The FDIC concurred with all eight recommendations in this report. The FDIC plans to complete all corrective actions by December 30, 2023.

Contents

BACKGROUND **2**

RESULTS **5**

Configuration of Wireless Network Devices 6

Finding #1: The FDIC's Policy Manager Used Outdated Protocols 6

Finding #2: The FDIC's Wi-Fi Operations Group Had Not Set Up or Secured Certain Wireless Devices Operating at FDIC Facilities 7

Wireless Signal Strength 9

Finding #3: The FDIC Does Not Evaluate the Strength of Wireless Signals and Networks Broadcasting Throughout Its Buildings and Leaking Outside of FDIC Facilities 9

Security Assessments and Authorizations 11

Finding #4: The FDIC Did Not Maintain a Current Authorization to Operate and Did Not Conduct Sufficient Continuous Controls Assessments for Its Wireless Networks 11

Vulnerability Scanning 13

Finding #5: Vulnerability Scans Did Not Include Certain Wireless Switches 13

Finding #6: The FDIC's Tools Did Not Support Credentialed Scans of Wireless Infrastructure Devices 14

Wireless Policies, Procedures, and Guidance 16

Finding #7: FDIC Wireless Policies and Procedures Were Missing Key Elements 16

FDIC COMMENTS AND OIG EVALUATION **19**

Appendices

1. Objective, Scope, and Methodology 20
2. Acronyms and Abbreviations 24
3. FDIC Comments 25
4. Summary of the FDIC's Corrective Actions 30

Figure

The FDIC's Wireless Network 3

December 13, 2022

Subject | ***Security Controls Over the FDIC's Wireless Networks***

The term, Wi-Fi, refers to wireless technology that allows internet enabled devices (laptops, tablets, and smartphones) to connect to wireless access points and communicate through a wireless network. Wi-Fi technology offers benefits to the Federal Deposit Insurance Corporation (FDIC), such as ease of deployment and installation and expanded network accessibility. However, Wi-Fi technology also presents security risks to FDIC systems and data.

The FDIC collects significant amounts of sensitive banking and personal information,[3] such as Personally Identifiable Information (PII).[4] PII may include the names, Social Security Numbers, and bank account numbers for FDIC employees and depositors of failed financial institutions. Sensitive information may include examination information, supervisory ratings, and Reports of Examination. Therefore, the FDIC must protect its data through effective security controls.

The most common security objectives for wireless networks, as identified by the National Institute of Standards and Technology (NIST), are the following:

- **Confidentiality**: Ensure that communication cannot be read by unauthorized parties;
- **Integrity**: Detect any intentional or unintentional changes to data that occur in transit;
- **Availability**: Ensure that devices and individuals can access a network or resources within a network; and
- **Access Controls**: Restrict the rights of devices or individuals to access a network or resources within a network.

The inherent weakness of Wi-Fi technology is that the signals are not bound by wires or walls and are therefore susceptible to signal interception and attack. According to NIST,[5] wireless networks face the following threats:

[3] According to FDIC Directive 1360.9, *Protecting Sensitive Information (April 30, 2007)*, sensitive information is any information, the loss, misuse, or unauthorized access to or modification of which could adversely impact the interests of the FDIC in carrying out its programs or the privacy to which individuals are entitled. PII is one type of sensitive information.
[4] According to FDIC Directive 1360.9, *Protecting Sensitive Information (April 30, 2007)*, PII is information about an individual maintained by the FDIC, which can be used to distinguish or trace that individual's identity.
[5] NIST Special Publication (SP) 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE802.11i* (February 2007).

Denial of Service: An attacker prevents or prohibits the normal use or management of networks or network devices.

Eavesdropping: An attacker passively monitors network communications for data, including authentication credentials (username and password).

Man-in-the-Middle: An attacker actively intercepts the path of communications between two legitimate parties, thereby obtaining authentication credentials and data. The attacker then masquerades as a legitimate party.

Masquerading: An attacker impersonates an authorized user and gains certain unauthorized privileges.

Message Replay: An attacker passively monitors transmissions and retransmits messages, acting as if the attacker were a legitimate user.

Traffic Analysis: An attacker passively monitors transmissions to identify communication patterns and participants.

As FDIC employees return to the office following the pandemic, the probability that an increased number of FDIC devices will be connected to the wireless networks magnifies the security risks described above.

The objective of our review was to determine whether the FDIC has implemented effective security controls to protect its wireless networks. We assessed the effectiveness of the FDIC's controls to protect its wireless networks in nine areas. Appendix 1 contains information about the objective, scope, methodology, and control areas tested.

BACKGROUND

The FDIC's Wireless Infrastructure

The FDIC's wireless infrastructure provides internet access for FDIC personnel, contractors, and guests across four networks:

1. **FDIC Corporate Network**: Internet access for FDIC-issued laptop computers;[6]

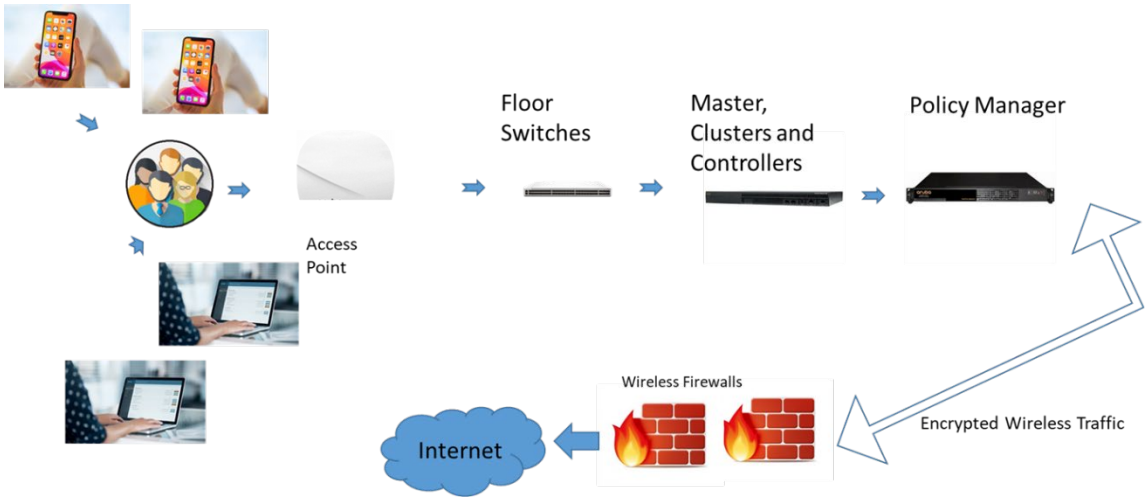
[6] The FDIC does not allow personal devices to enroll in its mobile device management program or connect to its Corporate Network.

2. **FDIC Mobile Network**: Internet access for FDIC-issued smartphones and tablets;
3. **FDIC Guest Network**: Internet access for all non-FDIC issued information technology devices; and
4. **Mobile Device Set-Up Network**: Used to set up FDIC-issued smartphones and tablets and only available to select individuals within the FDIC.

To access these networks, between January and November 2019, the FDIC installed about 1,200 wireless access points throughout its Headquarters buildings, regional offices, and field offices.[7] In August 2019, as part of the wireless expansion project, the FDIC began decommissioning certain legacy wireless devices and deployed the new FDIC Mobile and FDIC Guest Networks. As of the date of this report, the legacy wireless devices have been decommissioned.

As illustrated in the Figure below, FDIC employees, contractors, and guests can use a wireless-capable device (laptop, tablet, or smartphone) to connect to one of the many wireless access points broadcasting throughout FDIC hallways, conference rooms, and other common areas.

Figure: The FDIC's Wireless Network



Source: Office of Inspector General (OIG) Contractor, TWM Associates, Inc.

[7] FDIC Headquarters buildings are located at: (1) 550 17th Street, NW, Washington, D.C.; (2) 1776 F Street NW, Washington, D.C.; (3) 3501 N. Fairfax Drive, Arlington, VA (referred to as Virginia Square and the Student Residence Center); and (4) 3701 N. Fairfax Drive, Arlington, VA. The FDIC also maintains seven regional/area offices and numerous field offices across the country.

FDIC employees and contractors may access the FDIC Corporate Network (for FDIC-issued laptops) and Mobile Network (for FDIC-issued tablets and smartphones) to use FDIC applications and view FDIC data on the wired FDIC production network.[8] The FDIC also has a Mobile Device Set-Up Network for setting up FDIC-issued smartphones and tablets.

Guests may only use the FDIC Guest Network to access the internet after input of a passphrase and acceptance of the FDIC's acceptable use policy. However, the FDIC does not know the identity of individuals accessing the FDIC Guest Network.

As illustrated above, these wireless networks are supported by infrastructure devices such as switches, controllers, and policy managers. Wireless switches (floor switches) allow wireless access points to communicate with the wireless controllers. In turn, wireless controllers (master, clusters and controllers) help prevent access to the FDIC's Corporate Network from unauthorized devices. Wireless controllers then communicate with the Policy Manager to enforce security policies for how users and devices connect to the wireless network. The wireless traffic on each of the FDIC's networks is encrypted in transit through the firewall[9] to the internet access requested.

Roles and Responsibilities

The FDIC's Chief Information Officer Organization (CIOO) oversees the wireless networks at the Agency. The CIOO consists of three component organizations: the Division of Information Technology (DIT), the Office of the Chief Information Security Officer (OCISO), and the Chief Data Officer staff. DIT has primary responsibility for the day-to-day operational support and management of the FDIC's information systems and IT infrastructure, including its wireless networks.

The Wi-Fi Operations Group within DIT has responsibility for managing the FDIC's wireless networks, including: (1) resolving wireless-related plans of action and milestones (POA&M); (2) reviewing Daily Wireless Operations Reports (failed login attempts and configuration changes); (3) managing incoming tickets related to Wi-Fi connectivity from client services; and (4) maintaining wireless software and hardware.

[8] The wired FDIC production network is where products and applications operate in a live environment for actual use by the customers or end users. The FDIC Corporate Network provides employees a wireless alternative to physically connecting to the wired FDIC production network.
[9] Data in transit is the transfer of data to other locations within or between computer systems. A firewall protects a network by acting as an intermediary between the internal network and outside traffic and decides whether to block or allow traffic based on a defined set of security rules.

The OCISO has primary responsibility for the planning, development, and implementation of the FDIC-wide information security program, including the security controls around the Agency's wireless networks.

The Vulnerability Management Team within OCISO has responsibility for vulnerability and compliance scanning and reporting, third-party penetration testing, and internal penetration testing. The vulnerability scanning and compliance responsibility involves scanning the enterprise for system vulnerabilities and compliance with established baselines. The technical security assessment team is responsible for assessing products and applications before they are deployed for use. The application compliance program analyzes the output of security testing and helps ensure that security requirements are identified during application development.

RESULTS

We found that the FDIC did not always have effective security controls in place for five of the nine control areas we reviewed: configuration of wireless network devices; security assessment and authorization; rogue access points and wireless signal strength; vulnerability scanning; and policies, procedures, and guidance. Specifically, the FDIC did not:

(1) Configure its Policy Manager in accordance with required Federal guidelines;

(2) Require that DIT's Wi-Fi Operations Group manage the set-up and configuration of all FDIC wireless devices;

(3) Have processes in place to examine and modify the signal strength of wireless devices/networks broadcasting throughout its buildings and leaking outside of FDIC facilities;

(4) Maintain a current Authorization to Operate (ATO) for its wireless network and did not conduct sufficient continuous monitoring testing activities to support the Agency's ongoing authorization;

(5) Include certain wireless infrastructure devices in its vulnerability scans;

(6) Use credentialed scans on wireless infrastructure devices; and

(7) Maintain policies and procedures to address key elements pertaining to the FDIC's wireless networks.

The FDIC faces significant risks based upon its current wireless practices and controls, including potential unauthorized access to the FDIC networks and insecure wireless devices broadcasting Wi-Fi signals. The FDIC had effective controls in place for the remaining four control areas related to physical access controls of wireless infrastructure devices, access control and encryption, monitoring of user

internet destinations on its wireless networks, and disabling of legacy wireless networks.

Configuration of Wireless Network Devices

Network configuration is the process of setting a network's controls, flow, and operation to support the network communication of an organization. This term incorporates multiple configuration and set-up processes on network hardware, software, and other supporting devices and components.

Finding #1: The FDIC's Policy Manager Used Outdated Protocols

A Policy Manager for wireless security allows an organization to connect new devices to its network in compliance with organizational security policies. The Policy Manager uses the Simple Network Management Protocol (SNMP)[10] setting for monitoring and managing network devices. The purpose of SNMP is to provide network devices, such as routers, servers, and printers a common language to communicate with each other, referred to as an SNMP community string. An SNMP community string is similar to a user ID or password that allows access, in this case to a device.

According to the Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA), prior SNMP versions (versions 1 and 2) offered less protection as the SNMP community string is in plain text and not encrypted. Using the versions 1 and 2 could allow an adversary to gain access to the network devices and potentially gain access to the FDIC and its data.

We found that the FDIC was using an SNMP version 2 configuration setting in the Policy Manager and did not configure its SNMP configuration setting to version 3 in accordance with Federal guidelines[11] and vendor guidelines[12] in a timely manner. In June 2017, DHS CISA issued an alert to notify agencies that SNMP version 3 should be the only version of SNMP employed by Government agencies, because it has the ability to authenticate and encrypt the SNMP community string. Vendor hardening guidelines dated October 2014 and January 2018, recommended that organizations use the SNMP version 3 for enhanced security through authentication and encryption.

[10] SNMP is an internet standard protocol used to monitor and manage network devices such as routers, switches, servers, firewalls, and wireless access points.
[11] Alert TA17-156A, Reducing the Risk of SNMP Abuse | CISA (https://www.cisa.gov/uscert/ncas/alerts/TA17-156A).
[12] Vendor guidelines provide recommended secure configuration settings for specific information technology platforms/products.

The FDIC incurred a significant delay in updating the SNMP configuration setting in its Policy Manager. The CIOO asserted that the delay occurred because the FDIC's monitoring tool was not able to monitor network devices that are configured for the SNMP version 3 protocol, including the Policy Manager. The FDIC did not update the configuration setting on the Policy Manager until October 2021 – more than 8 months after the OIG had identified the issue for the CIOO, and more than 7 years after version 3 had already become available. The FDIC did not take this action for about 4 years after DHS CISA had instructed Government agencies to use version 3.

Additionally, the FDIC's Wi-Fi Operations Group did not create a POA&M regarding the Policy Manager to follow the DHS CISA alert recommended best practices for SNMP protocols. The FDIC's inaction was inconsistent with the creation of a POA&M (4148) regarding use of SNMP version 3 for a different vendor in July 2014. POA&Ms assist in identifying, assessing, prioritizing, and monitoring the progress of corrective actions pertaining to identified security vulnerabilities. POA&Ms also describe the resources required to accomplish remediation tasks and milestones for completion. A POA&M would have required the CIOO to assign a risk level to the potential security weaknesses associated with the SNMP version 2 protocol configuration setting on the Policy Manager and address the weaknesses within prescribed timeframes associated with the assigned risk level.

Recommendation
We recommend that the CIOO:

1. Ensure that wireless security weaknesses are consistently documented in POA&Ms and updated accordingly.

Finding #2: The FDIC's Wi-Fi Operations Group Had Not Set Up or Secured Certain Wireless Devices Operating at FDIC Facilities

During our walkthrough of the FDIC's Headquarters buildings in March 2021, we identified several wireless devices broadcasting wireless signals that were not configured and placed in operation by the FDIC's Wi-Fi Operations Group. These devices included printers, audio/visual devices, and Smart Boards[13] within FDIC spaces.

NIST SP 800-53, Revision 4,[14] AC-18, *Wireless Access*, recommends that an organization clearly define the roles of agency officials responsible for configuration and implementation of wireless devices. Further, the organization should establish implementation guidance, as well as configuration and connection requirements for

[13] A Smart Board is a whiteboard that connects to a computer, allowing users to interact with its screen.
[14] Our fieldwork was conducted using NIST SP 800-53, Revision 4, which was in effect at the time, but has since been updated to Revision 5, which became effective in September 2021.

each type of wireless access. Finally, the organization should authorize each type of wireless access prior to allowing such connections.

The FDIC's Wi-Fi Operations Group believed that it was not responsible for the configuration and set-up of these Wi-Fi capable devices. Further, the FDIC's Wi-Fi Operations Group stated that it had inspected a selection of wireless-enabled devices we identified during our walkthrough and determined that they were not connected to the wired FDIC production network. The FDIC's Wi-Fi Operations Group also asserted that there were additional monitoring controls to detect and terminate unauthorized devices that try to connect to the wired FDIC production network. Further, there were no policies or procedures that state which FDIC component is responsible for the configuration/set-up of Wi-Fi capable devices.

The wireless settings for devices were not set up by the FDIC's Wi-Fi Operations Group, and they pose a security risk. These devices were set up by other FDIC divisions and offices, and they did not coordinate with the Wi-Fi Operations Group on the security risks and settings on these wireless devices. Therefore, the FDIC's Wi-Fi Operations Group was not aware of these devices, even though some were transmitting without protection (encryption), and it is not clear what procedures were followed in order to set up these devices.

Devices such as Smart Boards and wireless printers can be connected to FDIC laptops that may contain PII and other sensitive information related to confidential bank examinations. The same FDIC laptops may be connected to the FDIC Corporate or FDIC Mobile Networks, which then provide a gateway for unauthorized individuals to potentially exploit and try to access FDIC data.[15]

Recommendation
We recommend that the CIOO:

2. Develop and implement a policy to review, approve, and centrally manage the configuration settings of current and future Wi-Fi enabled devices in FDIC facilities, before set-up and subsequent updates.

[15] Our review did not include testing exploits associated with wireless devices or mitigation of such risks.

Wireless Signal Strength

Finding #3: The FDIC Does Not Evaluate the Strength of Wireless Signals and Networks Broadcasting Throughout Its Buildings and Leaking Outside of FDIC Facilities

The FDIC did not have a process to determine if signal strengths on wireless networks or devices should be reduced or disabled. Wireless devices and networks broadcast communication signals to send data to other wireless devices, or to connect to an existing network through a wireless access point.

NIST SP 800-53, Revision 4, AC-18 (5) recommends that organizations select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of the organization-controlled boundaries. To address this vulnerability, an organization may adjust the signal strength or power of wireless transmissions outside its boundaries in order to limit unauthorized access.

We found that:

- The FDIC's Guest Network broadcasting from within the Headquarters Buildings was accessible outside of the perimeter of the buildings due to signal leakage;
- Numerous wireless access points with an FDIC label were broadcasting throughout the floors of the Headquarters buildings;
- FDIC devices, including printers[16] and Smart Boards, were broadcasting throughout and outside the Headquarters buildings; and
- The FDIC Mobile Device Set-Up network was picked up on eight floors in FDIC buildings, even though an FDIC official informed us that it was intended only for one floor.

We provided the FDIC with detailed information about the wireless access points wherein we had identified concerns over vulnerabilities.[17] In response, the Wi-Fi Operations Group stated its belief that decreasing signal strength on wireless devices could affect performance, and that there are controls in place which would help prevent these signals from being exploited; they did not believe that the risk was significant. The FDIC, however, did not provide any documentation to demonstrate

[16] During our fieldwork, the CIOO examined a subset of the FDIC printers we found broadcasting wireless signals and notified us that it had turned off the wireless functionality on four of the printers.
[17] Our review did not include an assessment of the wireless access points to determine if they pose a security vulnerability to the FDIC.

any analysis of the effect of signal strength at FDIC Headquarters facilities on performance.

In addition, the FDIC had previously acknowledged the security risk from signal leakage in a POA&M in 2013 (POA&M #3460). The POA&M was created because testers were able to connect to the (b) (7)(E) Guest[18] Network from outside of the building. The POA&M stated that while signal spill is difficult to eliminate, any amount of signal spill poses a security risk. Specifically, the POA&M states that this signal spill allows a potential hacker to connect to the (b) (7)(E) wireless network without physically entering the FDIC building. In November 2020, the testers recommended that the FDIC examine the pattern of signal dispersion within and outside the FDIC (b) (7)(E) and tune the broadcast signal appropriately. The FDIC did examine the recommendation of the testers and determined that the FDIC could not further reduce the signal without affecting the signal strength inside of the building. In November 2020, the FDIC Chief Information Officer signed and approved an Acceptance of Risk (AR)[19] for the signal spill at the (b) (7)(E) until September 2023.

Wireless devices that are broadcasting beyond their intended range may allow a hacker to intercept the wireless signal and scan the network to gather information that can be used in a hack.[20] Examples of attacks that utilize scanning methods include eavesdropping and traffic analysis. In these types of attacks, a hacker accesses the wireless network and monitors the network attempting to obtain various data regarding participants using the network, types of data and communications on the network, if encryption is used, and authentication credentials for users (username and password). Therefore, while wireless signals cannot be completely contained due to their inherent nature, reducing the signal strength as much as possible will minimize the risk to the FDIC's internal network.

Recommendations

We recommend that the CIOO:

3. Conduct a review of FDIC wireless devices and identify those that should not be broadcasting inside and leaking outside the buildings and take appropriate mitigation measures.

4. Develop and implement a process to regularly examine FDIC wireless devices and their broadcast areas in order to determine appropriate mitigation measures.

[18] POA&M 3460 was limited to the (b) (7)(E), and the FDIC provided no indication that it had analyzed spillage in other FDIC buildings and facilities.
[19] An Acceptance of Risk (AR) is used when a control weakness cannot be remediated for a valid business or technical reason. The AR is documented and signed by the CIO.
[20] Our review did not include a detailed assessment of the wireless access points identified.

Security Assessments and Authorizations

The security assessment and authorization of wireless networks is important given that such networks are vulnerable to unauthorized access and attacks. The purpose of a network security assessment is to keep networks, devices, and data safe and secure by discovering any information security weaknesses before they may be exploited by adversaries.

Finding #4: The FDIC Did Not Maintain a Current Authorization to Operate and Did Not Conduct Sufficient Continuous Controls Assessments for Its Wireless Networks

The FDIC had not updated its *Data Communications (DCOM) General Support System (GSS) Authorization to Operate (ATO)* from 2011, relating to the wireless infrastructure expansion in 2019. Further, the FDIC's continuous monitoring activities did not include testing of the configuration settings on the wireless infrastructure devices, such as switches, controllers, and policy managers.

Authorization to Operate

The ATO is an organization's official recognition and acceptance of the implemented controls and risks associated with a system's security posture. NIST SP 800-53, Revision 4, CA-6, *Authorization*, recommends that authorizing officials issue existing authorizations of systems based on data and information generated from continuous monitoring programs and update authorizations as needed.

In 2011, the FDIC issued an ATO for the DCOM GSS, which stated that a new ATO would be required if the system underwent a "significant change." In addition, the FDIC's *Security and Privacy Impact Process Guide* (issued by the OCISO) stated that retirement of a system is considered a "significant change." We found, however, that the FDIC did not update the ATO in 2019 when the legacy wireless infrastructure was retired.

During our fieldwork, we brought this matter to the attention of the FDIC and in January 2022, the FDIC provided us with an updated DCOM ATO. While the updated DCOM ATO addressed the portion of our finding related to it being outdated, the CIOO still needs to ensure that there are sufficient continuous monitoring activities to support the ATO and ongoing authorization of the wireless infrastructure.

Continuous Controls Assessments

The FDIC's Security Controls Assessment Methodology ("Methodology") contains a set of processes for the ongoing assessment and monitoring of information systems. According to the Methodology, wireless controls (including wireless configuration settings, processes, and procedures) were categorized as "Critical" and therefore were to be assessed annually.[21] The Methodology required the Assessment Team to conduct testing of the management, operational, and technical security controls for the system.

According to the System Security Plan, all DCOM GSS configuration settings should be documented in either a Secure Baseline Configuration Guide or a system build document, which are stored in a restricted SharePoint site. In addition, NIST SP 800-53, Revision 4, CM-6, *Configuration Settings*,[22] recommends that organizations establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements.

During our review, the CIOO stated that the FDIC had not created Secure Baseline Configuration Guides. Further, the CIOO stated that in the absence of Secure Baseline Configuration Guides, vendor hardening guidelines are used to test the configuration settings of the software and hardware. The vendor hardening guidelines recommended, for example, configurations for locking down services (such as SNMP and encryption); locking down access (for example administrators and users); and system monitoring (audit trails and rogue access points).

We found that the FDIC did not fully test security configurations on wireless infrastructure devices during its DCOM Security and Privacy Control Assessments in both 2020 and 2021. The *DCOM System Security and Privacy Control Assessment Report*, dated May 1, 2020, reported that "wireless access is provided by other components of DCOM not in scope for this assessment." The *Security and Privacy Control Assessment (SCA) – DCOM System, Appendix B: Test Results*, dated

[21] In the April 2020, FDIC Security and Privacy Control Assessment Methodology, version 1.0, both *Wireless Access* (AC-18) and *Configuration Settings* (CM-6) controls were categorized as "critical." The revised (January 2022) FDIC Security and Privacy Controls Methodology, version 2.4, provided after fieldwork was completed, categorized both AC-18 and CM-6 as low risk. This change requires wireless access controls to be tested within a 5-year period versus annually.

[22] According to NIST SP 800-53, Revision 4, CM-6, common secure configurations (also referred to as security configuration checklists, lockdown and hardening guidelines, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations, including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, Federal agencies, and other organizations in the public and private sectors.

April 28, 2021, indicated that the FDIC only examined the Acceptable Use Policy (AUP) and System Security Plan for completeness. The FDIC verified that encryption was enabled, but the FDIC did not provide support that it had actually tested the other wireless configuration settings, processes, and procedures based on vendor hardening guidelines.

The FDIC's security control assessment activities did not satisfy its annual security control assessment methodology requirements for assessing wireless controls that the FDIC deemed as "critical" during this timeframe. As a result, the FDIC did not fully assess if wireless networks were adequately hardened and configurations were secure.

Recommendation
We recommend that the CIOO:

5. Develop and provide training to appropriate personnel on the use of vendor hardening guidelines in conducting controls testing.

Vulnerability Scanning

Vulnerability scanning is the process of identifying security weaknesses and flaws in systems and software. Such scanning is an integral component of a software vulnerability management program to protect the organization from breaches and exposure of sensitive data. These programs gauge security readiness and minimize risk; vulnerability scanning is a critical tool in the cybersecurity toolbox.

Finding #5: Vulnerability Scans Did Not Include Certain Wireless Switches

We found that the FDIC's vulnerability scanning of its wireless infrastructure did not include certain switches on the FDIC systems. Switches are intermediaries between the wired access points and the wireless infrastructure allowing them to send traffic back and forth.

NIST SP 800-53, Revision 4, RA-5, *Vulnerability Monitoring and Scanning*, recommends that organizations monitor and scan for vulnerabilities in systems and hosted applications.[23] The FDIC conducts vulnerability scans on wireless switches and other wireless infrastructure devices, such as controllers and policy managers on a weekly basis. These scans help the FDIC identify vulnerabilities and misconfigurations that could allow an attacker to compromise the wireless network. If vulnerabilities are found, an alert is sent to the appropriate FDIC officials for further review.

[23] Hosted applications are applications that are accessed through the internet instead of internal servers.

We judgmentally sampled 10 of 56 wireless switches and reviewed the vulnerability scanning report for the week of March 23, 2021. We determined that two wireless switches were missing from the vulnerability scan results we reviewed.

In response to our concern, the FDIC's OCISO Vulnerability Management Team stated that it is common for a switch not to make it into a scan, and scans are run multiple times each month to mitigate this risk. The OCISO representatives explained that a switch may not be identified during a scan if it is turned off or malfunctioning. Upon further examination, the FDIC demonstrated that one of the missing switches was included in a subsequent vulnerability scan report of June 30, 2021, and the other switch was included in the vulnerability scan report of August 6, 2021.

While multiple scans may mitigate some risk, the FDIC did not have a process to regularly review scan results in order to ensure that all wireless infrastructure devices are being scanned. Based on documentation provided by the FDIC, we determined that the two switches missing from the vulnerability scanning report conducted on March 23, 2021 were not included in a vulnerability scan for about 2 to 5 months later. By not scanning every wireless infrastructure device, the FDIC may miss potential security exposures. During the course of our review, the CIOO stated that it would implement procedures to provide inventory lists to its Vulnerability Management Team when there are changes, such as additions and decommissioning of systems.

Recommendation
We recommend that the CIOO:

6. Develop and implement a process to regularly reconcile vulnerability scanning results to the inventory list of wireless infrastructure devices, so as to ensure that all devices are included in the FDIC's vulnerability scans.

Finding #6: The FDIC's Tools Did Not Support Credentialed Scans of Wireless Infrastructure Devices

We found that the FDIC did not perform credentialed scans of its wireless infrastructure devices due to incompatibilities between the FDIC's vulnerability scanning tool and its wireless infrastructure components.

A credentialed scan uses credentials to log into the system that provides insight into software vulnerabilities. Specifically, credentialed scans require logging in with validated user credentials, thereby providing a holistic view of the environment, including configuration weaknesses, missing patches, and similar vulnerabilities. By

contrast, non-credentialed scans provide an external view of the environment and, therefore, do not require credentials and do not get trusted access to the systems they are scanning.

NIST SP 800-53, Revision 4, RA-5b, *Vulnerability Monitoring and Scanning*, recommends that organizations employ vulnerability scanning tools and techniques that use standards for enumerating platforms, software flaws, and improper configurations. While NIST does not require organizations to employ credentialed scanning, the vendor of the scanning tool used by the FDIC states that credentialed scanning must be used to avoid incomplete or inaccurate system assessments.

Under the FDIC's Enterprise Security Operations Section, the Vulnerability Assessment Team runs a non-credentialed scan to identify software flaws and improper configuration in the software for wireless infrastructure devices.

During the course of our review, the FDIC explored credentialed scanning methods with a third-party vendor. However, the third-party vendor's scanning tool was incompatible with the FDIC's models of switches and prevented the use of automated credentialed scans. In the absence of the ability to conduct automated credentialed scans, the FDIC should consider other methods to enhance its vulnerability scanning process for wireless infrastructure devices.

Using credentialed scans, or an equivalent alternative, would improve the security of wireless infrastructure devices because they can identify vulnerabilities in the software, evaluate password policy, enumerate USB devices, and check antivirus software configurations and other activities much more thoroughly than a non-credentialed scan. For example, as discussed in our first finding related to misconfiguration of the Policy Manager, the Policy Manager SNMP setting was not configured to SNMP version 3 as required. This misconfiguration could have been detected by a credentialed scan.

Recommendation

We recommend that the CIOO:

7. Resolve incompatibilities between the third-party vendor's scanning tool and FDIC wireless infrastructure components, or conduct an analysis to identify viable alternatives for FDIC wireless infrastructure components and the associated level of effort and costs to enhance the vulnerability scanning process.

Wireless Policies, Procedures, and Guidance

Policies and procedures play an important role in the effective implementation of the enterprise-wide information security programs within every organization. Current policies, procedures, and guidance help to ensure that employees and contractor personnel implement security controls and practices in a proper, consistent, and disciplined manner.[24]

Finding #7: FDIC Wireless Policies and Procedures Were Missing Key Elements

We found that the FDIC's policies and procedures related to the wireless infrastructure did not address key aspects of managing its wireless data communications, roles, and responsibilities.

According to the Government Accountability Office's *Standards for Internal Control in the Federal Government* (September 2014), management must design and implement an effective internal control system. An important component of effective internal control is establishing control activities through policies and procedures to achieve objectives and respond to risks. Further, management should periodically review policies, procedures, and related control activities for continued relevance and effectiveness in achieving the entity's objectives or addressing related risks. FDIC Directive 4010.3, *Enterprise Risk Management and Internal Control Program* (October 2018), requires FDIC Divisions and Offices to regularly monitor and update policies and procedures to ensure strong controls are in place and risks have been addressed.

We found that the FDIC had implemented some organizational-wide IT policies and procedures that address topics applicable to the wireless networks, including the acceptable use of IT resources, POA&M management, network version control, and patch management.[25] However, these policies and procedures did not address key aspects of wireless data communications, roles, and responsibilities, such as:

- Roles and responsibilities of the CIOO's Wi-Fi Operations Group;[26]
- Procedures and timeliness requirements for remediating wireless access equipment alerts (for example, malfunctioning equipment);

[24] See FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* (March 2006).
[25] These policies and procedures include FDIC Directive 1300.4, *Acceptable Use Policy for FDIC Information Systems* (April 2017)*; POA&M Management and Acceptance of Risk Process, v. 1.3* (January 2021); *FDIC's Network Version Control Standard Operating Procedure, v. 1 2* (February 2020)*;* and *CIOO's Patch Management Standard Operating Procedure* (April 2019).
[26] As of July 1, 2022, the Wi-Fi Operations Group consisted of three individuals.

- Standards for configuration settings (FDIC-developed hardening guidelines which may be based on vendor practices) for wireless infrastructure devices, including the Controllers and Policy Manager;
- Requirements for updating wireless inventory records;
- Tracking of remediation activities that are not formalized as POA&Ms; and
- Rogue access point detection (the FDIC subsequently issued a standard operating procedure to address rogue access point detection, after completion of our fieldwork).

A rogue access point is a wireless access point that has been installed on a network without the consent of the network's administrator. These rogue access points broadcast wireless signals that hackers could connect to and use in their attempt to gain entry to the FDIC's network. Once on the network, an attacker could attempt to access FDIC systems and data. Because rogue access signals may be using no protection or limited protection, they can be used to attempt to bypass normal security procedures such as access management controls, which become easy targets for attackers to exploit.

We identified numerous wireless signals with FDIC in the name broadcasting throughout FDIC buildings. While the FDIC has monitoring in place for the wireless signals broadcasting, it had not applied classification labels to identify if the signal is a valid FDIC signal, neighboring non-rogue signal, or is being broadcast from a potential rogue access point.[27] In April 2022, FDIC personnel provided the OIG with a listing of potential rogue access point alerts that occurred between March 9, 2021 and February 28, 2022. The listing identified various signals, but the signals were not classified as valid, neighboring non-rogue, or rogue.

During our review, the FDIC stated that it did not see the need to investigate wireless signals broadcasting in its space that were not from the four FDIC wireless networks.[28] However, subsequent to completion of our fieldwork, the CIOO issued *DIT Wifi Rogue AP Detection SOP* [Standard Operating Procedure] (March 7, 2022). The purpose of this standard operating procedure is to describe the steps that need to be taken when the Wireless Intrusion Detection System detects a potential rogue signal.

[27] Per vendor documentation, a valid access point is one that is part of the environment. An interfering access point is seen in the environment, but it is not connected to the wired network (for example, a neighboring non-rogue signal from a nearby building). A rogue access point is an unauthorized access point.
[28] The FDIC's wireless infrastructure provides internet access for FDIC personnel, contractors, and guests across four networks: (1) FDIC Corporate, (2) FDIC Mobile, (3) FDIC Guest, and (4) Mobile Device Set-up networks.

In addition, the FDIC's policies did not address the following requirements pertaining to wireless user agreements:[29]

- Prohibitions on dual connections (for example, a laptop connected to a wireless and wired network at the same time);
- Prohibitions on peer-to-peer file sharing software;
- Requirements for installing antivirus software and keeping it current and up-to-date; and
- Privacy implications (no right to privacy) for users when using the FDIC's wireless data communications and how that is communicated.

Without documented policies and procedures, configuration standards, roles and responsibilities, and comprehensive user agreements, tasks may not be completed or not completed in a timely or appropriate manner. In addition, wireless infrastructure devices may be configured in a manner that makes them more susceptible to security risks from attackers trying to gain unauthorized entry into the FDIC internal network. Lastly, without clear guidelines in wireless user agreements, FDIC employees, contractors, and guests may not be fully aware of prohibited activities when using the FDIC wireless networks.

Recommendation

We recommend that the CIOO:

8. Develop, update, and implement wireless policies, procedures, and standards that reflect the FDIC's current business practices and key aspects of wireless data communications, roles and responsibilities, and acceptable use agreements.

[29] Wireless user agreements include the AUPs that guests must acknowledge before using the FDIC Guest Network and rules of behavior that FDIC employees and contractors must agree to before using FDIC IT resources.

FDIC COMMENTS AND OIG EVALUATION

The FDIC's Chief Information Officer (CIO) and Chief Information Security Officer (CISO) provided a written response, dated November 22, 2022, to a draft of the report. The response is presented in its entirety beginning on page 25. In the response, the CIO and CISO concurred with the report's recommendations. The recommendations will remain open until we confirm that corrective actions have been completed and are responsive. A summary of the FDIC's corrective actions begins on page 30.

Objective

The objective of our review was to determine whether the FDIC implemented effective security controls to protect its wireless networks.

We performed our work remotely and on-site in (b) (7)(E) from June 2021 through February 2022. We performed building walk-throughs at the (b) (7)(E). 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* (Silver Book). 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

We assessed the effectiveness of the FDIC's wireless infrastructure controls in nine security control areas generally covered by NIST SP 800-53, Rev 4:

Selected Wireless Control Areas	Definition
1. Policies, procedures, and guidance	NIST SP 800-53, Rev.4, AC-18, *Wireless Access*, recommends that organizations establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and authorize each type of wireless access to the system* prior to allowing such connections.
2. Disabling legacy wireless networks	NIST SP 800-53, Rev. 4, CM-3, *Configuration Change Control*, recommends configuration change control for organizational systems that includes disposition of system changes, including system upgrades and modifications.
3. Configuration of the wireless network devices	NIST SP 800-53, Rev.4, CM-6, *Configuration Settings*, recommends that organizations establish and document configuration settings for components employed within systems that reflect the most restrictive mode consistent with operational requirements; implement the configuration settings; identify, document, and approve any deviations; and monitor and control changes to the configuration settings.

4.	Access controls; encryption	NIST SP 800-53, Rev. 4, AC-1, *Policies and Procedures*, recommends that organizations develop, document, and disseminate access control policies, and review these policies on a periodic basis. NIST SP 800-53, Rev.4, AC-18(1), *Wireless Access*, recommends that organizations use authentication and encryption to protect wireless access to their systems.
5.	Patching and vulnerability scanning	NIST SP 800-53, Rev. 4, SI-2, *Flaw Remediation*, recommends that organizations identify, report, and correct system flaws within defined timeframes as part of the configuration management process. NIST SP 800-53, Rev. 4, RA-5, *Vulnerability Scanning*, recommends that organizations monitor and scan for vulnerabilities in systems and employ vulnerability tools and techniques.
6.	Wireless activity monitoring	NIST SP 800-53, Rev.4, AC-2, *Account Management*, recommends that organizations monitor the use of accounts. AC-2(12), Account Management, specifically requires monitoring for atypical account usage. NIST SP 800-53, Rev. 4, AU-2 requires event logging with specifications for event types and rationale for why event types are required for logging.
7.	Physical access for wireless devices	NIST SP 800-53, Rev. 4, PE-2, *Physical Access Authorizations*, recommends that organizations allow only authorized access to the facility where the system resides, and require appropriate credentials.
8.	Security assessment and authorization of wireless networks	NIST SP 800-53, Rev. 4, CA-6, *Authorization*, recommends that organizations authorize systems to operate and update authorizations based on an entity-defined frequency. NIST SP 800-53, Rev. 4, CA-7, *Continuous Monitoring*, recommends that organizations perform ongoing control assessments in accordance with their defined continuous monitoring strategy.
9.	Potential rogue access points and wireless signal strength	NIST SP 800-53, Rev. 4, SI-4(14), *Wireless Intrusion Detection*, recommends that organizations use a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the wireless system. NIST SP 800-53, Rev. 4, SI-4(22), *Unauthorized Network Services*, recommends that organizations perform monitoring to detect network services that have not been authorized or approved. These unauthorized or unapproved services may be unreliable or serve as malicious rogues for valid services. NIST SP 800-53, Rev. 4, AC-18-5, *Wireless Access | Antennas / Transmission power levels*, recommends that organizations select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of the organization-controlled boundaries. Some actions that may be taken to limit unauthorized use of wireless communications outside of organization-controlled boundaries include reducing the power of wireless transmissions so that transmissions are less likely to emit a signal that can be captured outside of the physical organization.

* System refers to the FDIC's wireless infrastructure.

We focused our testing related to the following four areas on the wireless infrastructure only at the FDIC's Headquarters buildings: (1) disabling the legacy wireless network, (2) configuring of the wireless network devices (primary controller devices and selected routers and firewalls), (3) physical access controls for wireless devices, and (4) rogue access points and wireless signal strength. To address our objective, the FDIC OIG engaged the professional services firm TWM Associates, Inc. to conduct a technical review that included the following procedures:

- Interviewed FDIC officials responsible for security controls over the wireless networks, including:
  - Wi-Fi Operations Group;
  - Vulnerability Management Team;
  - Network Services Unit; and
  - Network Operations Center.

- Identified and reviewed applicable Federal guidance, including:
  - NIST SP 800-53, Rev.4; and
  - Government Accountability Office's *Standards for Internal Control in the Federal Government* (Green Book) (September 2014).

- Reviewed FDIC policies and guidance related to the wireless infrastructure, including:
  - FDIC's *Acceptable Use Policy for FDIC Information Technology* (2017);
  - FDIC's *Plans of Action and Milestones (POA&M) and Acceptance of Risk Processes*, *v1.3* (2021);
  - FDIC's *Government Risk and Compliance (GRC) Plan of Action & Milestones (POA&M) Standard Operating Procedures, Version 1.0* (2020);
  - FDIC's *Network Version Control Standard Operating Procedure* (2020);
  - FDIC's *CIOO Patch Management SOP* (2019);
  - *DIT Wifi Rogue AP Detection SOP* (2022);
  - FDIC Circular 1360.10, *Corporate Password Standards* (2003);
  - FDIC Circular 1360.15, *Access Control for Information Technology Resources* (2009);
  - FDIC Circular 1360.16, *Mandatory Information Security Awareness Training* (2002); and
  - FDIC Circular, 1360.9, *Protecting Sensitive Information (2007)*.

- Considered the following Treasury Inspector General for Tax Administration and the U.S. Department of the Interior Inspector General Reports:
  - Treasury Inspector General for Tax Administration, *Improvements are Needed to Ensure Wireless Networks are Secure* (2020-20-63) (September 21, 2020); and

  - U.S. Department of the Interior Inspector General, *Evil Twins, Eavesdropping, and Password Cracking: How the Office of Inspector General Successfully Attacked the U.S. Department of Interior's Wireless Networks* (2018-ITA-020) (September 2020).

- Reviewed the following OIG reports:
  - *The FDIC's Information Security Program–2020* (FDIC OIG AUD-21-001) (October 2020); and *The FDIC's Information Security Program – 2021* (FDIC OIG AUD-22-001).
  - *The FDIC's Physical Security Risk Management Process* (FDIC OIG EVAL-19-001) (April 2019).

- Selected a random sample of three employee badges to determine if physical access control to wireless infrastructure devices was in place.

- Selected a random sample of three wireless controllers to determine if their configuration settings were appropriate.

- Selected a random sample of 10 wireless switches to determine if they were included in vulnerability scans.

- Selected a random sample of 25 wireless network signals broadcasting from the FDIC's access points to determine if they were included in the wireless access inventory.

- Conducted technical assessments to discover:
  - Wireless connections and broadcast strength/weaknesses;
  - Potential rogue wireless devices; and
  - Presence of legacy FDIC networks.

- Conducted technical evaluations to assess configuration settings for:
  - Wireless controllers and associated devices;
  - Firewalls;
  - Wireless network switches; and
  - Wireless communication controls.

- Reviewed the FDIC Risk Inventory to identify FDIC risks related to the objective.

Acronyms and Abbreviations

AR	Acceptance of Risk
ATO	Authorization to Operate
AUP	Acceptable Use Policy
CIOO	Chief Information Officer Organization
CISA	Cybersecurity & Infrastructure Security Agency
DCOM	Data Communications
DHS	Department of Homeland Security
DIT	Division of Information Technology
FDIC	Federal Deposit Insurance Corporation
FIPS	Federal Information Processing Standards
GSS	General Support System
NIST	National Institute of Standards and Technology
OCISO	Office of the Chief Information Security Officer
OIG	Office of Inspector General
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedure

NONPUBLIC//FDIC BUSINESS

Federal Deposit Insurance Corporation
Chief Information Officer Organization

November 22, 2022

To: Terry L. Gibson
Assistant Inspector General for Audits, Evaluations and Cyber

From: Sylvia W. Burns
SYLVIA BURNS Digitally signed by SYLVIA BURNS Date: 2022.11.22 11:01:04 -05'00'
Chief Information Officer, Chief Privacy Officer and
Director, Division of Information Technology

Zachary N. Brown
ZACHARY BROWN Digitally signed by ZACHARY BROWN Date: 2022.11.22 10:52:32 -05'00'
Chief Information Security Officer

Subject: Management Response to the Office of Inspector General's Draft Report, Entitled *Security Controls Over the FDIC's Wireless Networks* (No. 2021-003)

Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft review report, entitled *Security Controls Over the FDIC's Wireless Networks.* The OIG issued the draft report on November 8, 2022. The objective of the review was to determine whether the FDIC had implemented effective security controls to protect its wireless networks. The FDIC has deployed secure wireless technology in its facilities to expand network access for employees, contractor personnel, and other authorized users, and to provide Internet access for FDIC visitors and guests.

In its report, the OIG concluded that the FDIC had effective controls in place for four of nine areas assessed (i.e., physical access controls of wireless devices, access control and encryption, monitoring of user internet destinations on wireless networks, and disabling legacy wireless networks). Notably, the OIG's review did not identify any instances of unauthorized access involving the FDIC's wireless networks. The OIG's report also stated that the FDIC did not comply, or partially complied, with practices recommended by the National Institute of Standards and Technology, and other Federal and FDIC guidance in the remaining five areas assessed. These areas pertain to configuration management, monitoring of wireless signal strength, security assessments and authorizations, vulnerability scanning, and documentation of policies, procedures, and guidance. The issues identified in the OIG's report represent opportunities for the FDIC to improve its security controls and practices related to wireless networks.

The report contains eight recommendations to the Chief Information Officer (CIO) to improve wireless security controls and practices. The CIOO concurs with all eight recommendations. A summary of our planned corrective actions and associated milestones follows.

MANAGEMENT RESPONSE

Recommendation 1 -

We recommend that the CIO:

1. Ensure that wireless security weaknesses are consistently documented in POA&Ms and updated accordingly.

   Management Decision: Concur

   Corrective Action: The CIOO will assess its current processes for recording vulnerabilities in POA&Ms and make updates, as appropriate, to ensure that wireless security weaknesses are consistently documented in POA&Ms.

   Estimated Completion Date: 06/30/2023

Recommendation 2 -

We recommend that the CIO:

2. Develop and implement a policy to review, approve, and centrally manage the configuration settings of current and future Wi-Fi enabled devices in FDIC facilities, before set-up and subsequent updates.

   Management Decision: Concur

   Corrective Action: The CIOO will develop and implement a policy that defines roles and responsibilities for reviewing, approving, and managing the configuration settings of Wi-Fi enabled devices in FDIC facilities.

   Estimated Completion Date: 09/30/2023

Recommendation 3 -

We recommend that the CIO:

3. Conduct a review of FDIC wireless devices and identify those that should not be broadcasting inside and leaking outside the buildings and take appropriate mitigation measures.

   Management Decision: Concur

   Corrective Action: The CIOO will inventory FDIC Wi-Fi-enabled devices and ensure those that should not be broadcasting are disabled and those broadcasting intentionally are properly configured.

   Estimated Completion Date: 12/30/2023

Recommendation 4 -

We recommend that the CIO:

4. Develop and implement a process to regularly examine FDIC wireless devices and their broadcast areas in order to determine appropriate mitigation measures.

   Management Decision: Concur

   Corrective Action: The CIOO will enhance continuous monitoring processes for the wireless network environment to ensure that appropriate security controls (including broadcast configurations) are in place and operating as intended.

   Estimated Completion Date: 12/30/2023

Recommendation 5 -

We recommend that the CIO:

5. Develop and provide training to appropriate personnel on the use of vendor hardening guidelines in conducting controls testing.

   Management Decision: Concur

   Corrective Action: The CIOO will develop and provide training to security control assessors on leveraging vendor hardening guidelines during security controls testing.

   Estimated Completion Date: 05/01/2023

Recommendation 6 -

We recommend that the CIO:

6. Develop and implement a process to regularly reconcile vulnerability scanning results to the inventory list of wireless infrastructure devices, so as to ensure that all devices are included in the FDIC's vulnerability scans.

   Management Decision: Concur

   Corrective Action: The CIOO will implement a process to report the inventory of wireless devices to Vulnerability Management on a recurring basis to help ensure all devices are included in vulnerability scans.

   Estimated Completion Date: 03/31/2023

Recommendation 7 -

We recommend that the CIO:

7. Resolve incompatibilities between the third-party vendor's scanning tool and FDIC wireless infrastructure components, or conduct an analysis to identify viable alternatives for FDIC wireless infrastructure components and the associated level of effort and costs to enhance the vulnerability scanning process.

   Management Decision: Concur

   Corrective Action: The CIOO will perform an analysis to determine whether a viable alternative for scanning wireless infrastructure components can be utilized.

   Estimated Completion Date: 12/30/2023

Recommendation 8 -

We recommend that the CIO:

8. Develop, update, and implement wireless policies, procedures, and standards that reflect the FDIC's current business practices and key aspects of wireless data communications, roles and responsibilities, and acceptable use agreements.

NONPUBLIC//FDIC BUSINESS

Management Decision: Concur

Corrective Action: The CIOO will assess the Wi-Fi Operations Manual and make any necessary changes to address gaps in policies, procedures, and acceptable use agreements.

Estimated Completion Date: 10/31/2023

If you have any questions regarding this response, please contact Kevin Dupuis, Acting Chief of the Policy, Audit, Compliance, and Risk Section, at kdupuis@FDIC.gov.

cc: E. Marshall Gentry, Director, Office of Risk Management and Internal Controls
Greg S. Kempic, Office of Risk Management and Internal Controls
Mark Mulholland, Deputy CIO for Management
Sanjeev Purohit, Acting Deputy CIO for Technology

5

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 will assess its current processes for recording vulnerabilities in POA&Ms and make updates, as appropriate, to ensure that wireless security weaknesses are consistently documented in POA&Ms.	June 30, 2023	$0	Yes	Open
2	The CIOO will develop and implement a policy that defines roles and responsibilities for reviewing, approving, and managing the configuration settings of Wi-Fi enabled devices in FDIC facilities.	September 30, 2023	$0	Yes	Open
3	The CIOO will inventory FDIC Wi-Fi-enabled devices and ensure those that should not be broadcasting are disabled and those broadcasting intentionally are properly configured.	December 30, 2023	$0	Yes	Open
4	The CIOO will enhance continuous monitoring processes for the wireless network environment to ensure that appropriate security controls (including broadcast configurations) are in place and operating as intended.	December 30, 2023	$0	Yes	Open
5	The CIOO will develop and provide training to security control assessors on leveraging vendor hardening guidelines during security controls testing.	May 1, 2023	$0	Yes	Open
6	The CIOO will implement a process to report the inventory of wireless devices to Vulnerability Management on a recurring basis to help ensure all devices are included in vulnerability scans.	March 31, 2023	$0	Yes	Open
7	The CIOO will perform an analysis to determine whether a viable alternative for scanning wireless infrastructure components can be utilized.	December 30, 2023	$0	Yes	Open

8	The CIOO will assess the Wi-Fi Operations Manual and make any necessary changes to address gaps in policies, procedures, and acceptable use agreements.	October 31, 2023	$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.