Concerns Related to the FDIC's Pending Authorization to Operate Its External Wireless Network Solution Cloud Service

August 2021 **AEC Memorandum 21-001**

Memorandum

Audits, Evaluations, and Cyber

☆☆☆☆☆☆☆☆

Integrity☆Independence☆Accuracy☆Objectivity☆Accountability

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

Date: August 17, 2021

Memorandum To: Sylvia W. Burns
Chief Information Officer and Chief Privacy Officer

/Signed/
From: Terry L. Gibson
Assistant Inspector General for Audits, Evaluations, and Cyber

Subject: **Management Advisory Memorandum |** Concerns Related to the FDIC's Pending Authorization to Operate Its External Wireless Network Solution Cloud Service **|** AEC Memorandum 21-001

While conducting our ongoing audit of *Security Controls Over FDIC Wireless Networks*, we identified concerns that require your prompt attention.[1] These concerns relate to the FDIC's pending Authorization to Operate (ATO)[2] its external wireless network solution cloud service (Wireless solution). The Wireless solution allows users to set up, monitor, and configure wireless networks through a cloud-based service.

The FDIC's Division of Resolutions and Receiverships (DRR) has used the Wireless solution[3] to set up secure wireless networks during bank closings. In addition, the FDIC's Corporate University (CU) has used the Wireless solution for examiner courses with a need for an external internet connection. Also, the FDIC's Division of Information Technology (DIT) has used the Wireless solution for setting up mobile devices.

Background

In 2017, the Chief Information Officer Organization (CIOO) assigned a project team to identify a technology solution to replace the FDIC's then-existing bank closing kits. The project team determined that the Wireless solution could provide greater functionality over the FDIC's existing wireless network technology. According to a DIT official, the project team presented the

[1] While the audit is being conducted in accordance with Generally Accepted Government Auditing Standards (Yellow Book), the work covered by this Memorandum 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 (https://www.pandemicoversight.gov/media/file/agile-products-toolkit0pdf), include independence, analysis, evidence review, indexing and referencing, legal review, and supervision.
[2] Authorization to Operate is a formal management decision given by a senior official to authorize operation of an information system and accept the risk to agency operations (including mission, functions, image, and reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of security and privacy controls. Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, July 2016.
[3] The Wireless solution contains a pre-configured, wireless system comprised of wireless devices such as firewalls and switches.

Wireless solution to the FDIC's former Technology Review Group,[4] and received approval to proceed with the solution. In December 2017, the FDIC paid $216,113 for wireless services and devices.

In February 2018, the project team presented the Wireless solution to the newly-formed Security and Enterprise Architecture Technical Advisory Board (SEATAB)[5] for approval to proceed with obtaining an ATO. SEATAB deferred a decision and asked that the project team address whether the Wireless solution was an externally-hosted solution (outsourced service) or a cloud-based solution. SEATAB also asked the project team to provide additional documentation related to the Wireless solution's applicability to other FDIC business processes, and an updated profile and architecture diagram.

In August 2018, the project team determined that the Wireless solution was a non-cloud outsourced service as they concluded that it did not fully meet the National Institute of Standards and Technology's (NIST) definition of a cloud solution.[6] Therefore, according to this determination by the project team, the FDIC's use of the Wireless solution did not require an ATO for its services, and instead, was subject to the CIOO's Outsourced Solution Assessment Methodology (OSAM).[7]

According to OSAM, while Federal guidance requires all information systems to be authorized to operate, this may not be feasible for all outsourced solutions given the nature of the solutions and the relationships with the vendors. We did not evaluate the determination by the project team that the Wireless solution was a non-cloud service because such issues were beyond the scope of our ongoing audit. Therefore, we do not have an understanding of how the project team reached their determination that the Wireless solution was a non-cloud based service and should be subject to OSAM.

In April 2019, DIT determined that it had completed the necessary OSAM processes to move the Wireless solution into the production environment for use. DRR first used the Wireless solution for a bank closing in October 2019. As of November 2020, the FDIC had spent over $1.2 million on the wireless services and devices.

Concerns

In December 2018, NIST released Special Publication 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. One of the purposes of the revision was to integrate security-related, supply chain risk management (SCRM) concepts into the Risk Management Framework (RMF). With the implementation of Revision 2 of the RMF, the OSAM was found to be partially redundant to the RMF process and was superseded by the new mandatory RMF SCRM

[4] The Technical Review Group was a governance body responsible for evaluating the introduction of new technologies to the FDIC's IT environment, including technical requirements, how the proposed technology met those requirements, and the impact the technology would have on the existing IT infrastructure.
[5] According to its charter, SEATAB serves as the governance body for the FDIC's Enterprise Architecture and any new technology introduced in the FDIC's environment. In addition, SEATAB absorbed the responsibilities of the Technical Review Group.
[6] The project team consulted with the Governance, Risk and Compliance (GRC) section prior to making its determination. As a result of the Office of the Chief Information Security Officer (OCISO) re-organization in February 2021, GRC was renamed the Cyber Risk Management (CRM) Section.
[7] OSAM was used to provide the FDIC with a consistent, well-informed, and ongoing security process for outsourced information systems and services.

obligations. As a result, in June 2020, the OCISO rescinded OSAM and determined that the Wireless solution would need to be subject to the NIST's RMF. The project team and GRC therefore initiated the ATO process for the Wireless solution's cloud service in August 2020. As part of the ATO process, the FDIC requires a security assessment in accordance with NIST guidance. The project team contacted the Wireless solution's vendor to request the necessary documentation to support the security assessment required for an ATO.

The vendor, however, was not able to provide sufficient documentation to support an ATO and informed the project team that a Federal Risk and Authorization Management Program (FedRAMP) authorization was in process for the Wireless solution.[8] Therefore, in order to complete the ATO process, the CIOO determined it would leverage the wireless vendor's FedRAMP authorization once it was completed.[8] As of January 2021, the ATO was put on hold pending the FedRAMP authorization. As of April 2021, according to a DIT Information Security Manager, the FedRAMP readiness assessment for the Wireless solution was delayed until July 2021[9] with a FedRAMP authorization expected approximately a year later, in July 2022.[10] According to DIT staff, the FDIC has not had a business need to use the Wireless solution since February 2020.

Although the CIOO followed the OSAM processes prior to placing the Wireless solution in operation, the CIOO has not been able to fully assess the risks and authorize the Wireless solution to operate in the FDIC's IT environment consistent with NIST guidance. Therefore, the CIOO should consider whether additional actions should be taken such as putting in place an acceptance of risk (AR)[11] for the Wireless solution pending the completion of the FedRAMP authorization process and ATO.[12]

In addition, it is important that the CRM is aware of all uses of the Wireless solution in the FDIC environment to ensure risks are fully evaluated as part of the AR and ATO processes, as applicable. The Chief of the CRM was not aware the Wireless solution was also used by CU and DIT.

[8] FedRAMP is a Government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP empowers agencies to use cloud technologies with an emphasis on security and protection of Federal information.

[9] As of July 23, 2021, the DIT Information Security Manager informed the OIG that the target date of July 2021 for the readiness assessment date is unlikely at this point and that the vendor is expected to provide an updated roadmap soon.

[10] The FedRAMP authorization process contains multiple steps. This includes a preparation step, which consists of a readiness assessment and a pre-authorization by a third-party organization to document the cloud service provider's capability to meet Federal security requirements. The process also includes an authorization step, which consists of a full security assessment by a third-party assessment organization.

[11] An AR is used to capture risk acceptance decisions by senior management related to security findings and other security weaknesses.

[12] An ATO is a management decision given by a senior official to authorize operation of an information system and accept the risk to agency operations, agency assets, individuals, other organizations, and the Nation based on the implementation of security and privacy controls.

FDIC Response

The FDIC's Chief Information Officer (CIO) and Chief Information Security Officer (CISO) provided a written response, dated August 10, 2021, to a draft of this memorandum addressing the OIG's concerns. The response is presented in its entirety in the Appendix.

Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990
Chief Information Officer

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

THROUGH: Sylvia W. Burns SYLVIA BURNS Digitally signed by SYLVIA BURNS Date: 2021.08.10 20:53:48 -04'00'
Chief Information Officer, Chief Privacy Officer & Director, DIT

FROM: Zachary N. Brown
Chief Information Security Officer ZACHARY BROWN Digitally signed by ZACHARY BROWN Date: 2021.08.10 20:55:59 -04'00'

SUBJECT: Management Response to the Advisory Memorandum Titled *Concerns Related to the FDIC's Pending Authorization to Operate Its External Wireless Network Solution Cloud Service | No. 2021-003*

DATE: August 10, 2021

Thank you for the opportunity to provide a written response to the Office of Inspector General's (OIG) Advisory Memorandum on the *Concerns Related to the FDIC's Pending Authorization to Operate Its External Wireless Network Solution Cloud Service*, issued July 27, 2021 (Advisory Memo). In the Advisory Memo, the OIG documented three primary concerns:

1. The wireless solution had not been authorized to operate in the FDIC's IT environment consistent with National Institute of Standards and Technology (NIST) guidance;
2. Additional risk mitigation actions should be considered pending the completion of an Authorization to Operate (ATO) for the wireless solution; and
3. The Cyber Risk Management (CRM) Section was not aware of all uses of the wireless solution.

Our response addresses each of these concerns.

Pending Authorization to Operate

As detailed in the Advisory Memo, the wireless solution was approved under the legacy Outsourced Solution Assessment Methodology (OSAM) process. In June 2020, the FDIC rescinded OSAM and all other legacy approval processes that did not align with the NIST Risk Management Framework (RMF). In doing so, the FDIC reinforced and clarified the comprehensive adoption of the RMF at the FDIC.

The FDIC is working to ensure that all of its systems, including the wireless solution cited in the Advisory Memo, align with the RMF. Toward this objective, the CIOO has made significant progress:

1. In April of 2020, OCISO launched the Cyber Security Assessment and Management (CSAM) system, a federal shared service offering hosted and operated by the Department of Justice, as the authoritative source for FDIC authorized systems and subsystems and to track and administer continuous monitoring of the information security and privacy controls of these systems. CSAM implementation revealed several legacy approvals that were outdated and not aligned to the state of the practice for federal information system authorizations. These revelations prompted the refinement and establishment of authoritative and logical FDIC system boundaries to allow for improved visibility and enhanced information risk management for the Corporation.
2. In June of 2020, as noted above, the CIO rescinded all legacy approval processes to reinforce and clarify the comprehensive adoption of the RMF at the FDIC. The FDIC Legal Division concurred with this decision.
3. In July of 2020, OCISO partnered with several Divisions to begin reviewing all pre-award procurements to ensure uniform application of information security and privacy requirements in systems, services, and components that are managed by contractors for or on behalf of the FDIC.
4. From July 2020 forward, OCISO has consistently applied the RMF authorization process to all new FDIC developments and deployments, as well as conducting initial authorizations of systems operating under legacy approvals, as needed, to support incremental deployments and releases.
5. In March of 2021, OCISO worked with the Division of Administration, Acquisition Services Branch (ASB), to issue the ASB Procurement Administrative Bulletin (PAB 2021-01) communicating changes to the Form 3700/60, Checklist for Information Security and Privacy Provisions/Clauses and instructions, to improve application and integration of information security and privacy into procurement actions. This made OCISO review of pre-award procurements under ASB's Acquisition Procedures, Guidance, and Information (PGI), permanent. It ensures that new contractor-operated FDIC systems include RMF authorization requirements, as appropriate.
6. From March 2021 to the present, OCISO has proactively engaged owners of operational systems to verify their status, reuse legacy approval documentation as much as possible, and update system information to understand how operational systems relate to other systems across the enterprise. This systems inventory review concluded that almost a third of the operational systems and subsystems with legacy approvals did not align to the current RMF.

Consider whether Additional actions are Warranted Pending an ATO

The Advisory Memo notes that, although the CIOO followed the OSAM processes prior to placing the wireless solution in operation, the CIOO has not been able to fully assess the risks and

authorize the wireless solution to operate in the FDIC's IT environment consistent with NIST guidance. Therefore, the CIOO should consider whether additional actions should be taken, such as putting in place an acceptance of risk (AR) for the wireless solution pending the completion of the FedRAMP authorization process and ATO.

On July 23, 2021, the CIOO formally acknowledged that there are FDIC systems operating under legacy approvals that do not fully align with the RMF. The CIOO did so by issuing a memo titled, *Acknowledgement of Systems Operating under Legacy Approvals*. Although significant progress has occurred to mature the FDIC's system authorization processes, (as described above) the CIOO recognized and documented a compelling need for the continued operation of systems authorized through legacy approvals, as work continues to bring all systems with legacy approvals under RMF authorization.

In the memo issued on July 23, 2021, the Chief Information Security Officer noted that it is essential that systems with legacy approvals remain operational as we bring them into alignment with the RMF to ensure that FDIC mission operations are not adversely impacted. The CISO also acknowledged conditions and controls that are in place to mitigate the risks associated with the continued operation of systems with legacy approvals:

1. Systems operated for or on behalf of the FDIC by contractors include contract clauses and provisions that hold the contractors responsible for information security and privacy requirements that were in place at the time the contract was awarded. Oversight Managers and Contracting Officers continue to be responsible for ensuring those requirements are met.
2. Subsystems with legacy approvals often inherit a number of the required NIST controls from the system to which they align, limiting risk from the overall unassessed controls to the FDIC.
3. Cloud systems that have a FEDRAMP authorization inherit many of the required NIST controls from the Cloud Service Provider (CSP), limiting risk from the overall unassessed controls to those designated as agency responsibility.
4. Systems and subsystems launched on FDIC premises were generally subject to technical security assessments or other reviews, were architected to operate inside protected network perimeters, and are subject to security monitoring.
5. OCISO Enterprise Security Operations proactively defends all FDIC systems and information from cyber threats using people, process, and technology that are applied commensurate with the relative risk to each system and aligned to the Corporation's risk appetite and tolerance levels.

With this memo, the FDIC Authorizing Official recorded the decision to allow the continued operation of the FDIC systems currently operating under legacy approvals. The OCISO is addressing each system via a risk-based process under its Legacy Approvals Action Plan.

Awareness of all Uses of the Wireless Solution

The Advisory Memo notes that it is important for personnel with RMF/System Authorization responsibilities to be aware of all uses of the wireless solution in the FDIC's environment to ensure that risks are fully evaluated as part of the Acceptance of Risk and ATO processes, as applicable. The OIG identified a lack of awareness that the wireless solution was used by Corporate University and the Division of Information Technology.

The CIOO acknowledges the importance of such awareness. Comprehensive adoption of the Risk Management Framework and the associated RMF-based Assessment and Authorization processes will ensure risks are fully evaluated. The assessment for the wireless solution is planned to occur following the solution's FedRAMP authorization, which is scheduled to occur in 2022, to ensure that use cases are known and stakeholders are informed.

While actions are ongoing to fully implement the RMF, the FDIC has approved the wireless solution to be used across all Divisions and Offices under a legacy approval process. Conditions and controls are in place to mitigate the risks associated with continued operation of this and other systems with legacy approvals, as was noted previously.

We appreciate your staff's time and effort and we expect the actions taken and planned will address the concerns noted in this advisory memorandum. The plan established by the FDIC to bring all systems into alignment with the RMF strikes the appropriate balance between risk management, operational necessity, and cost efficiency to bring systems operating under legacy approvals into conformance with the RMF.

Cybersecurity is critical to the FDIC's ability to carry out its mission of maintaining stability and public confidence in the nation's financial system. It continues to be a top priority at the FDIC.

cc: Zachary Brown, Chief Information Security Officer
Montrice Yakimov, Chief, IT Risk, Governance, and Policy Section, ESB
Shannon Dahn, OCISO Lead on FDIC Legacy Approvals Plan

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.