The FDIC's Security Controls Over Microsoft Windows Active Directory

March 2023 **No. AUD-23-002**

Audit Report

Audits, Evaluations, and Cyber

☆☆☆☆☆☆☆☆

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

Integrity☆Independence☆Accuracy☆Objectivity☆Accountability

NOTICE

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

The FDIC's Security Controls Over Microsoft Windows Active Directory

The Federal Deposit Insurance Corporation (FDIC) relies heavily on information systems containing sensitive data to carry out its responsibilities. To ensure that only individuals with a business need are allowed access, the FDIC uses Active Directory (AD) to centrally manage user identification, authentication, and authorization. AD infrastructure is an attractive target for attackers because the same functionality that grants legitimate users access to systems and data can be hijacked by malicious actors for nefarious purposes. Therefore, it is paramount for the FDIC to ensure that it is adequately protecting its AD infrastructure. The objective of our audit was to assess the effectiveness of controls for securing and managing the Windows AD to protect the FDIC's network, systems, and data. The FDIC Office of Inspector General (OIG) engaged the professional services firm of Cotton & Company Assurance and Advisory, LLC (Cotton) to conduct this audit.

Results

We determined that the FDIC had not fully established and implemented effective controls for securing and managing the Windows AD to protect the FDIC's network, systems, and data in 7 of the 12 areas we assessed. Specifically, we found that the FDIC should improve controls in the following areas:

1. **Password Management:** The FDIC configured hundreds of accounts [redacted] or password changes. In addition, multiple privileged users (a) reused their passwords; (b) shared their passwords across multiple accounts; and (c) did not change their passwords for over a year.
2. **Account Configuration:** Privileged accounts were configured with excessive privileges. Such privileges were not justified as necessary and could allow attackers to inflict significant damage if these accounts were compromised.
3. **Access Management:** The FDIC account deletion setting did not remove over 900 users after they exceeded the required thresholds related to account inactivity. In addition, the FDIC suspended its automated account inactivity setting for a month in late 2021 without compensating controls.
4. **Privileged Account Management:** Three FDIC users held privileged access for almost a year after the access was no longer required for their positions.

5. **Windows Operating System Maintenance:** Several servers and a workstation in the (b) (7)(E) domain were running unsupported versions of the Windows or Windows Server Operating System.
6. **AD Policies and Procedures:** The AD Operations Manual included inaccurate information about the FDIC's implementation of AD.
7. **Audit Logging and Monitoring:** The FDIC did not enable performance monitoring on two domain controllers supporting its AD infrastructure.

The FDIC's ineffective AD security controls could pose significant risks to FDIC data and systems. In addition, the cumulative impact of these weaknesses could result in an attacker covertly obtaining administrative privileges to the FDIC's AD, potentially allowing the attacker to obtain, manipulate, or delete data across the network, causing serious damage to the FDIC and its mission and reputation. Moreover, account misconfigurations by the FDIC may provide FDIC employees and contractors unnecessary elevated privileges on the FDIC's network.

We found that the FDIC had effective controls in the remaining five control areas we assessed related to configuration management, contingency planning, patch management, vulnerability remediation, and defining key AD points of contact.

Recommendations

We are making 15 recommendations to improve AD security controls in the 7 areas listed above. Specifically, we recommend that the FDIC provide password training and implement controls to monitor and track password usage. In addition, we recommend that the FDIC remove unnecessary elevated domain privileges and regularly review and remediate any misconfigured accounts. Further, we recommend that the FDIC only use supported versions of Windows Operating Systems. Finally, we recommend that the FDIC issue and maintain a current AD Operations Manual.

The FDIC concurred with all 15 recommendations in this report. The FDIC plans to complete all corrective actions by March 31, 2024.

Contents

Part I

****

Report by Cotton & Company Assurance
and Advisory, LLC

FEDERAL DEPOSIT INSURANCE CORPORATION'S SECURITY CONTROLS OVER MICROSOFT WINDOWS ACTIVE DIRECTORY

AUDIT REPORT

MARCH 15, 2023

Cotton, A Sikich Company
333 John Carlyle Street, Suite 500
Alexandria, Virginia 22314
703.836.6701 | 703.836.0941, fax
lschwartz@cottoncpa.com | www.cottoncpa.com

Table of Contents

Cotton
A SIKICH. COMPANY

333 John Carlyle Street, Suite 500 | Alexandria, VA 22314
P: 703.836.6701 | F: 703.836.0941 | www.cottoncpa.com

Jason M. Yovich
Deputy Assistant Inspector General for Audits, Evaluations, and Cyber
Office of Inspector General
Federal Deposit Insurance Corporation

Subject: Audit of the Federal Deposit Insurance Corporation's Security Controls Over Microsoft Windows Active Directory

Cotton & Company Assurance and Advisory, LLC (Cotton) is pleased to submit the attached report detailing the results of our performance audit of the Federal Deposit Insurance Corporation's (FDIC) Security Controls Over Microsoft Windows Active Directory. The FDIC Office of Inspector General engaged Cotton to conduct this performance audit. Cotton performed the work from September 2020 through March 2023.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards promulgated by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Sincerely,

(b) (6)

Simon Lee CISA, CISSP
Director

Introduction

The Federal Deposit Insurance Corporation (FDIC) relies heavily on information systems to carry out its responsibilities of insuring deposits; examining and supervising financial institutions for safety, soundness, and consumer protection; making large and complex financial institutions resolvable; and managing receiverships. These systems contain sensitive information, such as Personally Identifiable Information, including names, Social Security Numbers, and bank account numbers for FDIC employees and depositors of failed financial institutions; confidential bank examination information, including supervisory ratings; and sensitive financial data, including credit card numbers.

The FDIC grants users access to FDIC information systems containing sensitive data. These users may include FDIC employees, contractors, and financial institution employees. To ensure that only individuals with a business need are allowed to access FDIC information systems and the data contained therein, the FDIC relies on automated controls to ensure users have proper identification, authentication, and authorization:

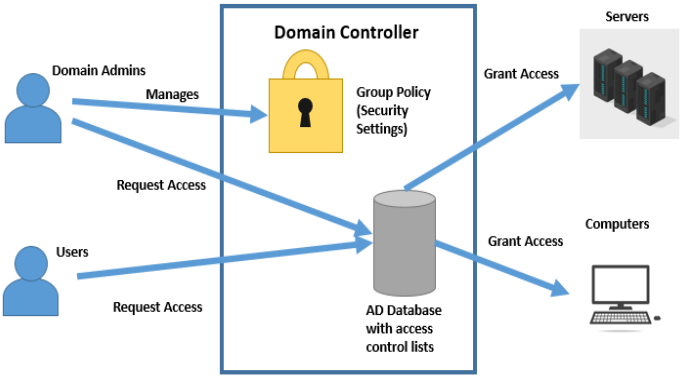
- **Identification:** The ability to uniquely identify a user of a system (often in the form of a User ID).
- **Authentication:** Verifying that a user is genuinely who that person claims to be. There are three common types of verification factors:
    1. Something only the user knows (such as a password or personal identification number);
    2. Something only the user has (such as a Personal Identity Verification [PIV] card or token); and
    3. Something the user is (such as fingerprints).

  Requiring two or more types of verification for access is called multi-factor authentication and generally provides more security than only requiring one type of authentication.
- **Authorization:** Determining that a user is only provided access to system resources for which the user is approved. For example, a general user will not have the same authorization as a system administrator.

Because implementing these automated controls can be complex due to the wide range of users and information systems, the FDIC manages these processes centrally across its network using a directory service. Active Directory (AD) is a commonly used directory service developed by the Microsoft Corporation that controls system access across an agency's network.

As illustrated in **Figure 1**, when a user attempts to access a resource (for example an application or a server[1]), the user's workstation will send a request to a server, called a domain controller.[2] Next, the domain controller determines whether the access is authorized, and then allows or rejects the request. The same check applies to each request by any user to any resource across the FDIC's network via AD. Additionally, the domain controller allows domain administrators to set security policies for different accounts via Group Policy.[3]

Figure 1: FDIC High-Level AD Infrastructure



Source: Cotton's analysis of the FDIC's AD structure.

The AD infrastructure, and especially its domain controllers, are attractive targets for attackers because it controls access to the FDIC's information systems and data. The same functionality that grants legitimate users access to systems to perform their duties can be hijacked by malicious actors for nefarious purposes. An attacker who obtains privileged access to AD can leverage it to access, control, or even destroy elements of the AD infrastructure and the applications that rely on it. Therefore, it is paramount for the FDIC to implement secure controls to ensure that it is adequately protecting its AD infrastructure.

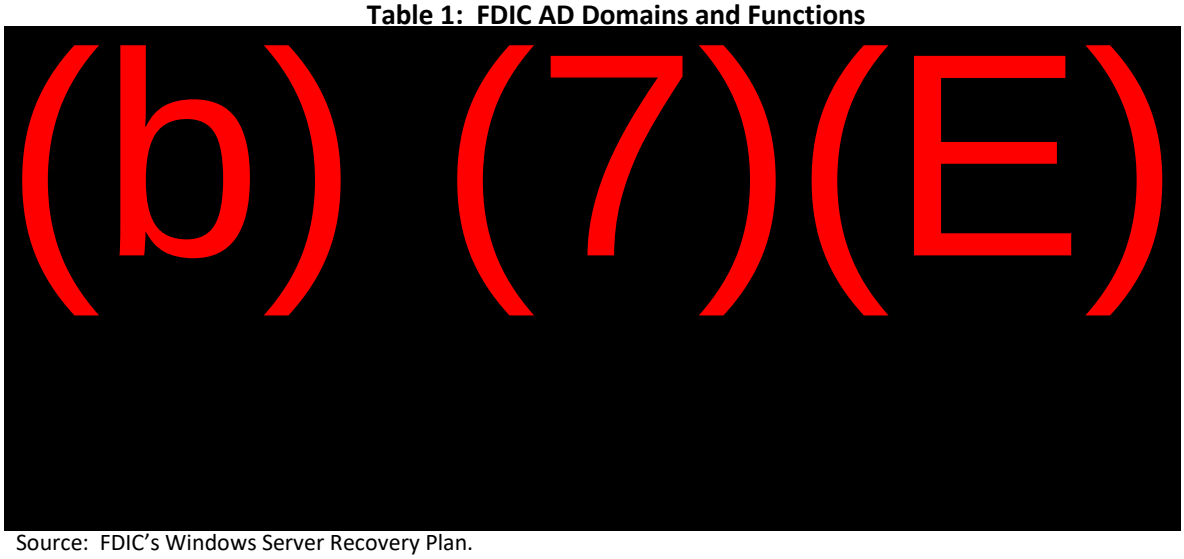
Background

FDIC Active Directory Implementation

AD allows administrators to logically organize an entity's resources (for example, computers and servers) into different domains. Each domain is supported by separate domain controllers. As shown in **Table 1** below, the FDIC's AD implementation consists of (b) (7)(E) domains that accommodate separate functions at the FDIC:

[1] According to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-123, *Guide to General Server Security*, a server is a device that provides one or more services for other hosts over a network as a primary function.
[2] A domain controller is a server that runs AD and responds to authentication requests on a network.
[3] Group Policy is a security tool that allows administrators to granularly define security policies for users and computers.

Table 1: FDIC AD Domains and Functions



Source: FDIC's Windows Server Recovery Plan.

[a] According to NIST SP 800-81-2, *Secure DNS Deployment Guide*, DNS is an engine that converts user-friendly domain names on the internet (for example, fdic.gov) into machine-readable Internet Protocol (IP) addresses (such as 172.30.128.27). IP addresses allow internet resources to be uniquely identified.

The (b) (7)(E) domains listed first (b) (7)(E) are the "production" domains and grant access to live systems. Among these domains, the (b) (7)(E) domain carries the highest risk as it contains most FDIC user accounts and supports most FDIC business functions. As a result, the FDIC holds the (b) (7)(E) domain to the highest control standards. The remaining (b) (7)(E) domains are development domains that do not control access to data used by the FDIC to perform its mission; therefore, they pose less risk to the FDIC.

Each domain contains multiple domain controllers to ensure that the failure of one will not interrupt authentication operations throughout the Agency. Access control lists between domain controllers in the same domain are automatically and regularly copied to ensure that any changes made to one are synchronized to all. The (b) (7)(E) domain contains the most domain controllers as it is used to authenticate all FDIC user accounts. There are separate domain controllers supporting the main FDIC offices in the Washington, D.C. region, the Regional Offices, and the FDIC Backup Data Center.

Roles and Responsibilities

Within the FDIC, the Chief Information Officer (CIO) has responsibility for Information Technology (IT) governance, investments, program management, and information security. The Chief Information Officer Organization (CIOO) maintains a Wintel[4] Operations Team, which is responsible for managing the FDIC's AD, to include adding and removing users and groups and implementing configuration changes. The Wintel Operations Team focuses on the FDIC's Cloud, Infrastructure & Platform Services that provide ongoing support to the FDIC's IT infrastructure, including all operating systems, cloud services, and the Backup Data Center.

[4] Wintel is commonly used to refer to computers that run the Windows operating system on an Intel processor.

AD Controls Assessed During the Audit

We assessed the effectiveness of the FDIC's controls to protect its AD in 12 areas.[5] We identified these areas based on our analysis of relevant NIST security standards and guidance, FDIC policy and guidance, Microsoft best practices, and government-wide security policy requirements. **Table 8** in **Appendix II** contains additional information about the AD control areas we tested and the associated criteria.

Audit Objective

The objective of this performance audit was to assess the effectiveness of controls for securing and managing the Windows Active Directory to protect the FDIC's network, systems, and data.

Audit Results

We determined that the FDIC had not fully established and implemented effective controls for securing and managing the Windows Active Directory to protect the FDIC's network, systems, and data in 7 of the 12 areas we assessed. Specifically, we found that the FDIC should improve controls in the following areas:

1. **Password Management**: The FDIC configured hundreds of accounts in the (b) (7)(E) and (b) (7)(E) domains that (b) (7)(E) or password changes. In addition, multiple privileged users (a) reused their passwords; (b) shared their passwords across multiple accounts; and (c) did not change their passwords for over a year. Privileged users are entrusted with a high degree of authority over support operations critical to a successful security program and have powerful privileges. If attackers compromise privileged user accounts, they could potentially manipulate operating system and security controls. As a result, privileged users need a higher degree of technical knowledge in effective security practices and implementation, and should be held to the highest standards.
2. **Account Configuration**: Privileged accounts were configured with excessive privileges. Such privileges were not justified as necessary and could allow attackers to inflict significant damage if these accounts were compromised. As a result, malicious actors could leverage the privileged account access to attack the network.
3. **Access Management**: The FDIC account deletion setting did not remove over 900 users after they exceeded the required thresholds related to account inactivity. In addition, the FDIC suspended its automated account inactivity setting for a month in late 2021 without compensating controls.
4. **Privileged Account Management**: Three FDIC users held privileged access for almost a year after the access was no longer required for their positions.
5. **Windows Operating System Maintenance**: Several servers and a workstation in the (b) (7)(E) domain were running unsupported versions of the Windows or Windows Server Operating System.
6. **AD Policies and Procedures**: The AD Operations Manual included inaccurate information about the FDIC's implementation of Active Directory.

[5] We also assessed the effectiveness of 12 internal control areas as described in **Table 7** in **Appendix II** that we deemed significant to the audit objective and relevant to the 12 AD control areas we tested.

7. **Audit Logging and Monitoring**: The FDIC did not enable performance monitoring on two domain controllers supporting its AD infrastructure.

The FDIC's ineffective AD security controls could pose significant risks to FDIC data and systems.[6] In addition, the cumulative impact of these weaknesses could result in an attacker covertly obtaining administrative privileges to the FDIC's AD, potentially allowing the attacker to obtain, manipulate, or delete data across the network, causing serious damage to the FDIC and its mission and reputation. Moreover, account misconfigurations by the FDIC may provide FDIC employees and contractors unnecessary elevated privileges on the FDIC's network.

We found that the FDIC had effective controls in the remaining five control areas we assessed related to configuration management, contingency planning, patch management, vulnerability remediation, and defining key AD points of contact.

We are making 15 recommendations to improve AD security controls in the 7 areas listed above.

Password Management

We found that the FDIC configured hundreds of accounts in the (b) (7)(E) and (b) (7)(E) domains that (b) (7)(E) [redacted] or not require password changes. In addition, numerous privileged users reused their passwords, used the same passwords across multiple accounts, or did not change their passwords for over a year. As stated above, privileged users should be held to the highest standards due to the powerful authorities and privileges entrusted to them. Password management weaknesses provide opportunities for attackers to obtain account access to FDIC systems and sensitive data. Such password weaknesses also heighten insider threat risk that may arise from an FDIC employee or contractor inappropriately obtaining a privileged user's credentials and misusing this access to compromise the confidentiality, availability, or integrity of the FDIC's systems and data.

FDIC Circular 1360.10, *Corporate Password Standards*, states that in the absence of more advanced access controls, passwords are the first line of defense to ensure that access to FDIC data is limited to only authorized users. The Circular establishes specific requirements for FDIC passwords, including:

- Passwords must have a minimum of eight characters (16 characters for administrators).
- Passwords must meet a complexity threshold by containing characters from three of the following four categories:
    - English uppercase letters,
    - English lowercase letters,
    - Arabic numerals, and
    - Punctuation and other special characters.
- New or changed passwords must differ from the previous 10 passwords established by a user.
- Passwords must be changed after 90 days.

[6] Identified risks related to the FDIC's Active Directory are not currently captured in the FDIC's Risk Inventory.

- Passwords must be stored only as encrypted hashes (a short string of letters and/or numbers)[7] rather than easily readable (plaintext) files.

To determine password compliance with FDIC Circular 1360.10, *Corporate Password Standards*, it was necessary to recover passwords across the (b) (7)(E) FDIC domains as part of our testing.[8] To perform our analysis, FDIC administrators provided a file containing hashes for all account passwords within the organization. Using this hash file,[9] we used a sophisticated cracking system to attempt to obtain the passwords.

Cracking is the process where an attacker attempts to recover the original password from the password hash. By design, a hashing algorithm will turn the same text into the same hash. Therefore, attackers would try to guess the password, and if their guess produces the same hash as the recovered password hash, it means they have successfully guessed the password. The most basic attack relies on brute force, whereby an attacker tries all possible combinations until they match the hash. However, an attacker can use more sophisticated forms of brute force to increase the likelihood of matching (for example, using words from a dictionary), especially if an agency has weak password policies.[10]

By having the hash file and using the cracking system, we were able to test password compliance by recovering nearly half of the passwords within the organization – approximately 47 percent (22,750 of 48,871 total passwords).[11] Our results of recovered passwords are summarized in **Table 2** below:

Table 2: Password Analysis Results

Type of Account	Password Length Requirement	Total Number of Passwords	Number of Passwords Recovered	Approximate Percentage
Users	Eight characters	48,554	22,711	47 percent
Privileged Users	Sixteen characters	317	39	12 percent

Source: Cotton analysis of passwords for 48,871 accounts.

We determined that the passwords recovered complied with FDIC password length and complexity requirements and only identified limited instances of shared common root words.[12] However, we noted the following practices for privileged user accounts that violated FDIC policies and/or rendered passwords subject to compromise:

[7] Systems should not store passwords in their original form. Instead, they store them as password hashes, which result from applying a one-way mathematical algorithm called a hash function to a password. A one-way algorithm converts the password into a unique string of characters that cannot be directly reverted back to a clear text password. The same text would always generate the same hash, and the hash function cannot be reversed to reveal the password.

[8] See Appendix II for a description of the testing method used to recover passwords.

[9] Obtaining a hash file would be difficult for an attacker. In order to extract the password hash file, an attacker would first need to gain access to a domain controller.

[10] The subcontractor's cracking system used a blend of proprietary and publicly accessible cracking software and advanced techniques. For this effort, the cracking system used custom rules and analytics to identify combinations of words and phrases that may likely be used as passwords. In addition, the cracking system approximated the results achievable based on the assumptions of an experienced attacker with a modest budget and roughly a one-week window in which to operate.

[11] Note that the FDIC's extensive use of multi-factor authentication means that having the password alone generally will not result in obtaining access to an account. However, using strong passwords remains a best practice in ensuring an effective control environment.

[12] A shared common root word is a fixed segment that remains the same within multiple passwords, to include an element that a user could more easily remember. Users could then keep this fixed segment while changing a different part of the password, such as a prefix, suffix, and/or a single character they could increment (e.g., from "a" to "b" or from "1" to "2") to fulfill password complexity requirements. Within (b) (7)(E) we identified instances of the most common 4 character string in only 1.74 percent of all passwords.

- Twelve privileged users with domain administrator accounts had not changed their password in more than a year.[13]
- Eighteen instances where a user used the same password for a lower privileged account as the user did for at least one higher privileged account.[14]
- Fifteen privileged users re-used at least 5 of their previous 10 passwords despite an automated setting in place to prevent users from re-using their last 10 passwords. (b) (7)(E)
- Four accounts reused passwords at least five times and shared a password with another privileged account.

In addition, we recovered approximately 12 percent (39 of 317) of the passwords for domain administrators, the highest privileged accounts in an AD implementation. Privileged users should be held to the highest standards due to the elevated authorities and privileges entrusted to them.

Finally, we inspected the password-relevant account configurations of all FDIC users across the (b) (7)(E) domains and noted numerous accounts with settings that did not comply with FDIC password policies. Specifically, (b) (7)(E) and some accounts were not required to change their passwords (see **Table 3**):

Table 3: FDIC Accounts with Non-Compliant Password Settings

(b) (7)(E)

Source: Cotton analysis of FDIC password settings from August 30, 2021 to November 18, 2021.

The CIOO officials asserted that these findings resulted from two factors. First, since individuals are responsible for creating and remembering their own passwords, they gravitate towards conveniences, including re-using passwords. Second, the CIOO had not defined nor consistently implemented least privilege[16] requirements at the account setting configuration level. CIOO officials stated their views that

[13] Although the password expiration setting is 90 days, we were not able to determine whether the accounts with expired passwords could actually be used to log in. Therefore, we judgmentally highlighted the instances with the highest risk – domain administrator accounts with passwords that had not been changed for a year.

[14] Privileged users hold at least two accounts: a "general user" account and at least one privileged account. Privileged accounts include domain administrator accounts and other administrator accounts. For the purpose of this report, an administrator account is considered lower privileged than a domain administrator account. We defined an instance as one of the following:

- A user using the same password for a general user account as an administrator or domain administrator account.
- A user using the same password for an administrator account and domain administrator account.

[15] (b) (7)(E)

[16] NIST SP 800-53, Rev. 4 (January 2015) recommends that organizations implement the security principle of "least privilege." The principle refers to the security objective of restricting user access to only those IT resources needed to perform official duties.

the non-compliant password settings in the [redacted] domain were acceptable in such a setting. In December 2021, after we discussed our findings with the FDIC CIOO, the CIOO initiated a deviation from the Secure Baseline Configuration Guide[17] to seek and obtain approval from the FDIC CIO and CIOO senior management of the exceptions for the [redacted] domain.

Re-using passwords across accounts with different privilege levels, not changing passwords for extended periods of time, and using the same password across different privileged accounts would violate security protocols and provide opportunities for persistent attackers to obtain account passwords. They could then use the passwords to access FDIC accounts and traverse the network and/or escalate privileges to compromise, exfiltrate, or deny access to FDIC data. This risk is exacerbated by instances where passwords are not required to be changed or [redacted]. Similarly, poor password practices by privileged users pose a heightened risk because their accounts are entrusted with a high degree of authority over support operations critical to a successful security program and have powerful privileges that enable attackers to manipulate operating system and security controls should they obtain access to the accounts.

Prior to our audit, the CIOO implemented a privileged account management tool that automatically generates and stores passwords for privileged users on an as-needed basis. In August 2021, the CIOO advised that it had also begun [redacted] to record a privileged user's actions when performing administrative duties to reduce the risk of unauthorized administrator actions. As of May 2022, the FDIC had implemented the feature for privileged access to servers but had not yet developed and implemented associated policies and procedures.

We recommend that the CIO:

1. Provide additional training to emphasize password requirements for privileged account users and communicate the effect of poor password practices, including those identified in this report.
2. Develop and implement controls to monitor and track password usage for privileged users and domain administrators to mitigate insecure password practices.
3. Approve and maintain Secure Baseline Configuration Guide deviations for accounts in the identified domain, as appropriate.
4. Develop and implement policies and procedures to automate the password creation and management process for privileged Active Directory accounts.

Account Configuration

The FDIC did not have effective processes for account configurations to ensure that permissions were aligned with the least privilege principle of restricting access to the minimum required for a user to perform their job responsibilities. Specifically, privileged accounts were configured with excessive privileges that would allow attackers to inflict significant damage if they were able to compromise these accounts. Accounts with excessive access permissions are attractive targets because compromising such elevated accounts would allow malicious actors to more easily attack the network.

[17] A Secure Baseline Configuration Guide is the FDIC implementation of a Security Configuration Checklist, which according to NIST, is a series of instructions/settings for configuring an IT product in accordance with the agency's IT security needs (https://www.nist.gov/programs-projects/security-configuration-checklists-commercial-it-products#:~:text=A%20security%20configuration%20checklist%20(also,identifying%20unauthorized%20changes%20to%20the).

Domain Administrator accounts have full control over the domain, including editing any permissions and configurations, and are necessary for administering AD. However, we identified 170 other privileged accounts[18] that were configured with elevated domain privileges that were not needed. For example, these elevated privileges included (b) (7)(E) and (b) (7)(E), which provide the following abilities:

- (b) (7)(E)
- (b) (7)(E)

Appendix I provides (b) (7)(E)

CIOO officials stated that they have not defined account permission settings to ensure that FDIC employees and contractors responsible for configuring accounts do so in accordance with the least privilege principle. The FDIC must ensure that user accounts are configured properly when they are initially set up, and that these accounts are monitored on a regular and frequent basis in order to identify misconfigurations susceptible to compromise by external and insider threats.

We recommend that the CIO:

5. Remove unnecessary elevated domain privileges for accounts across all FDIC domains.
6. Develop and implement permission settings and configurations for privileged accounts that are aligned with the principle of least privilege.
7. Develop and implement monitoring mechanisms to regularly review privileged account settings and configurations and remediate any misconfigured accounts.

Access Management

Though the FDIC creates new AD accounts and performs account reviews on a regular basis, access management improvements are needed. Specifically, the FDIC suspended its automated inactive user deactivation setting for one month in late 2021 without implementing any compensating controls. The FDIC account deletion setting also did not remove over 900 inactive accounts in (b) (7)(E) domains as of April 29, 2021, after they exceeded each domain's prescribed inactivity threshold. Inactive user accounts and accounts of separated users pose an increased security risk to the FDIC because they provide unnecessary access points onto the network and additional targets for attackers.

FDIC Circular 1360.15, *Access Control for Information Technology Resources*, dated March 2011, requires

[18] Tables 5 (34 accounts) and 6 (157 accounts) in Appendix I show 191 accounts total. There were 21 accounts that appeared in multiple categories, resulting in a total of 170 accounts.

[19] When designing an Active Directory logical structure, administrators can group a subset of resources within a domain into an "organizational unit" and administer them separately. Doing so allows for more granular administration.

that access to IT resources be given for legitimate business purposes only and after proper authorization has been provided. In addition, NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Information Systems and Organizations* (January 2015), recommends that agencies (1) define and document the types of accounts allowed and specifically prohibited for use within the system; and (2) create, enable, modify, disable, and remove accounts in accordance with agency requirements.

We noted deficiencies within the FDIC's disabling and deletion procedures for accounts that were no longer needed.

Accounts Not Disabled or Deleted in a Timely Manner

The FDIC automatically disables user access and removes accounts that have been inactive for an extended period. Additionally, in accordance with FDIC Circular 1360.15 and NIST SP 800-53, Rev. 4, the FDIC can manually disable accounts when they are no longer needed (for example, when a user departs the FDIC). The disabling and deletion[20] thresholds vary depending on the domain and its business requirements (see **Table 4** for thresholds).

Table 4: FDIC Account Disabling and Deletion Thresholds

Domain	Disabling Threshold (in Days)	Deletion Threshold (in Days)
(b) (7)(E)	30	120
(b) (7)(E)	90	120
(b) (7)(E)	365	395
(b) (7)(E)	90	120

Source: FDIC Policy on Inactive Windows User Accounts.

We found that on April 29, 2021, 919 inactive user accounts remained within AD even though the users last logged in prior to the threshold deadlines for account deletion. The number of user accounts per domain are shown below:

- (b) (7)(E) **Domain:** 548 users last logged in over 120 days ago
- (b) (7)(E) **Domain:** 300 users last logged in over 120 days ago
- (b) (7)(E) **Domain:** 33 users last logged in over 395 days ago
- (b) (7)(E) **Domain:** 38 users last logged in over 120 days ago

Further, we determined that as of November 15, 2021, 33 user accounts in the (b) (7)(E) domain remained enabled despite not having logged in for over 30 days, thus violating the 30-day inactivity disabling threshold. The 33 accounts had last logged in between 33 and 1,370 days prior.[21]

The inactive user accounts identified in (b) (7)(E) were a result of the FDIC temporarily[22] suspending an automated control used for disabling and removing inactive accounts to address an operational issue with its account management system. The FDIC had turned off the setting that enforced the inactivity thresholds because some accounts were inadvertently disabled or deleted. However, the FDIC did not

[20] A disabled account is unable to be accessed, but can be reactivated by an administrator. A deleted account is permanently removed.
[21] Although the upper range of inactivity (1,370 days) suggests that that the setting was inoperable for longer than the temporary setting suspension noted in the cause, we performed additional work on these accounts and noted that these accounts were manually reactivated through a new user request and then deactivated by the inactivity setting because they never logged in.
[22] The setting was not active from the last week of October 2021 to the last week of November 2021.

employ compensating controls to replace the functionality of the automated control when it was not in use. Inactive user accounts and accounts belonging to separated users pose a security risk to the FDIC computing environment. These accounts, which no longer have a business need, could be used to inappropriately access network resources without authorization, which can result in compromise or theft of FDIC data.

Also, we determined that the FDIC had implemented a certification schedule to review accounts on a regular basis. We tested a subset of certifications (to include at least one account from each of the (b) (7)(E) domains: (b) (7)(E)) and determined that certifications were performed in a timely manner and included all relevant users.

We recommend that the CIO:

8. Identify inactive user accounts and disable or delete them in accordance with FDIC policy.
9. Design and implement mitigating controls to address occurrences where the automated inactivity setting is inoperable.

Privileged Account Management

We found that the FDIC had effective processes for provisioning[23] and approving Domain Administrators and Wintel Administrators. However, the FDIC must make improvements to the management of privileged accounts. Specifically, based on our analysis of all (b) (7)(E) administrators in April and November 2021, three FDIC users held privileged access for almost a year after the access was no longer required for their position. Retaining access when it is no longer needed increases the risk of unauthorized access to FDIC systems and data.

Privileged users hold privileged accounts in addition to their general user account. Accordingly, the FDIC employs a Role-Based Access Control (RBAC) system in which it defines a list of roles, each granting access to one or more system actions that a user can perform (called "entitlements"). FDIC users who need system access are given one or more roles based on their business need. CIOO management developed documents that list the names of the roles, the owner of the roles, the account types, the entitlements to which roles have access, and a justification/description for each role. Privileged accounts are defined as such because they hold multiple roles that are considered privileged.

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Information Systems and Organizations*, states that restricting privileged accounts to specific personnel or roles prevents day-to-day users from accessing privileged information or privileged functions. Privileged accounts within the FDIC include (b) :

- (b) (7)(E) **account:** Limited to domain administrators
- (b) (7)(E) **account:** Desktop administrator, including the Help Desk
- (b) (7) **account:** Any other type of elevated access

We noted that the accounts were appropriately provisioned and were properly (b) (7)(E) . We also noted that new privileged users were appropriately approved prior

[23] Provisioning refers to the processes for creating accounts and providing those accounts with proper access to system resources.

to obtaining access. However, we identified three individuals who held excessive privileges and accesses, as described below.

Obsolete Roles Led to Users Holding Excessive Access

The FDIC conducts reviews of individuals assigned to roles and entitlements defined in its RBAC documents to determine if modifications are needed due to changing business needs. Specifically, the owners of each role, as defined in the RBAC documents, review the list of users that hold the role to determine whether they are correct. The RBAC documents are not intended to be static and roles may be added, changed, or removed based on business need. Additionally, roles are not mutually exclusive and may have overlapping entitlements. We noted that these circumstances resulted in three instances in 2021 where users held two roles (henceforth titled "Role A" and "Role B") that granted identical administrative access when no longer needed.

In April and November 2021, the FDIC determined that the three users should retain access to Role A and be removed from Role B since the users no longer had a business need for the role. However, since both roles provided the three users the same entitlements, they retained those entitlements despite the requested removal of one of the roles. Additionally, in May 2021, the FDIC eliminated the need for Role A since it was obsolete but did not update the RBAC document accordingly. Consequently, the three users retained excessive administrative privileges to FDIC systems and data due to an erroneous determination by the Role A Role Owner in November 2021 that they needed access to an obsolete role.

This underscores the importance of an effective process to review roles and associated entitlements to ensure that they are allocated appropriately and removed in a timely manner when no longer needed. Without an effective review process, users may have excessive administrative privileges to FDIC systems and data.

We recommend that the CIO:

10. Develop and implement a process to regularly evaluate the roles to determine whether they are still needed or duplicative of other roles.
11. Develop and implement a process to reconcile conflicting certification determinations for duplicative roles.

Windows Operating System Maintenance

Ineffective Processes for Operating System Maintenance

The FDIC did not update the Windows Operating System on certain AD components in the (b) (7)(E) domain in a timely manner. In August 2021, six servers and one workstation were running operating systems for which the vendor ended support in January 2020, approximately 18 months earlier.[24] NIST SP 800-53, Rev. 4, Control SA-22, *Unsupported System Components*, states that agencies should replace information system components when support for the components is no longer available from the vendor.

The CIOO stated that six servers were not decommissioned prior to the end of the support date because

[24] The servers were running Windows Server 2008 R2 Enterprise Service Pack 1 and one workstation was running Windows 7 Enterprise Service Pack 1.

they were part of an ongoing effort to upgrade voice and video equipment. Additionally, the workstation was decommissioned in January 2022 because it was no longer needed.

Support for information system components includes software patches, firmware updates, replacement parts, and maintenance contracts. Unsupported components provide a substantial opportunity for attackers to exploit new weaknesses discovered in the currently installed components. Additionally, unsupported AD components may affect the availability and performance of FDIC networks and systems in support of the FDIC's mission.

We recommend that the CIO:

12. Update and implement procedures to proactively update or replace operating systems before vendor support ends.

Active Directory Policies and Procedures

Active Directory Operations Manual is Out of Date

The CIOO documents its key procedures regarding AD administration in the AD Domain Services 2012 Operations Manual (Operations Manual). However, we found that it contained outdated information about the AD infrastructure and related controls. Specifically, the Operations Manual included:

(1) Outdated domains and domain controllers;
(2) Log management software decommissioned in 2014 that has since been replaced; and
(3) No acknowledgement that a trust relationship[25] existed between two AD domains – (b) (7)(E) [redacted].

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.

CIOO officials stated that they had not prioritized updates to the Operations Manual because they were in the process of developing a new Operations Manual to support an ongoing effort to upgrade the AD infrastructure from Windows Server 2012 to 2019. The new manual is scheduled to be published in June 2023.

Agencies rely on policies and procedures to document institutional knowledge and reduce the risk from the departure of knowledgeable individuals. Without accurate information in the Operations Manual, key AD personnel may act upon incorrect information to administer AD, increasing the risk that controls

[25] A trust relationship exists between two domains when users authenticated in one domain (the trusted domain) can access the resources of another domain (the trusting domain).

may not be applied appropriately and impacting the confidentiality, integrity, and availability of FDIC systems and data.

We recommend that the CIO:

13. Issue a current, updated Active Directory Operations Manual.
14. Develop and implement procedures to regularly update the Active Directory Operations Manual to reflect the current structure and practices.

Audit Logging and Monitoring

The FDIC established automated processes[26] to identify suspicious events impacting the AD environment and notify the appropriate personnel. However, the FDIC needs to make improvements to its logging and monitoring activities. Specifically, the FDIC did not enable performance monitoring[27] on two domain controllers supporting its AD infrastructure. Without performance monitoring, AD administrators may not have a full picture of the health of each domain controller.

According to NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Information Systems and Organizations*, agencies are responsible for identifying and responding to significant security events. These requirements include identifying the events that it considers relevant to security and developing mechanisms to track when the events take place. This tracking is commonly accomplished using audit logs, which are records of events occurring within an information system or network. Agencies must then be able to review the logs for indications of inappropriate or unusual activity. To maintain the usefulness of the audit logs, agencies must ensure that they are protected from unauthorized access, modification, and deletion and retained for a sufficient period.

We noted that the FDIC developed adequate mechanisms to identify suspicious events affecting the AD environment and notify the appropriate personnel, reviewed its alert triggers for effectiveness, and retained audit logs in accordance with retention requirements.

However, we found that the FDIC did not fully enable performance monitoring on its AD infrastructure.

Performance Monitoring Not Enabled on Two Domain Controllers

The CIOO uses a performance monitoring tool to monitor the overall health of the AD system and provide alerts for critical performance issues, including service availability. However, the tool was not monitoring 2 of the [redacted] domain controllers in the FDIC's AD infrastructure. The two domain controllers were in this state for about one month prior to remediation in November 2021.

If the performance monitoring tool is not implemented on all domain controllers, AD administrators may not have a full picture of the health of each domain controller, increasing the risk that signs of compromise or unplanned downtime may be missed.

[26] These automated processes include tools for security event and information monitoring, Windows event activity logging, and audit log management.
[27] Performance monitoring refers to the monitoring of the overall operational health of a system, including whether it is using computing resources efficiently and whether it is available to all users who need it.

We recommend that the CIO:

15. Develop and implement a process to monitor all domain controllers and ensure that any exceptions are addressed timely.

Configuration Management

The FDIC established configuration management processes for the AD infrastructure. We determined that the Windows Server 2012 R2 configuration supporting AD complied with NIST SP 800-70, Rev. 4, *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers,* and FDIC Policy 16-005.

Contingency Planning

The FDIC established processes to develop and test system contingency plans for the AD infrastructure. We determined that components supporting AD were failed over to its Backup Datacenter,[28] tested, failed back,[29] and tested with passing results in accordance with NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*.

Patch Management

The FDIC developed a Wintel Patching schedule for the AD infrastructure. We determined that Windows patches were appropriately implemented across all relevant AD servers for the 4 months tested, in accordance with NIST SP 800-40, Rev. 3, *Guide to Enterprise Patch Management Technologies*.

Vulnerability Remediation

The FDIC established processes to prioritize and monitor risks and the progress of corrective actions related to the AD infrastructure. We determined that all AD-related Plans of Action and Milestones included sufficient evidence supporting closure, and the most recent vulnerability scan included all domain controllers, in accordance with NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Information Systems and Organizations*.

Defining Key Active Directory Points of Contact

The FDIC established processes to restrict privileged access to a limited set of personnel, and we determined that privileged AD responsibilities were granted sparingly with oversight by the CIOO's Cloud, Infrastructure & Platform Services personnel.

[28] The FDIC operates two datacenters. Under normal circumstances, the primary datacenter is responsible for processing FDIC data. However, if the primary datacenter is partially or fully inoperable due to a contingency event, the backup datacenter assumes processing responsibilities, helping ensure the continued operation of the FDIC's systems. The two datacenters are located in different geographical locations to minimize the risk of an event impacting both datacenters.

[29] A failover is the process whereby a backup system takes over processing responsibilities in case the primary system goes down. A failback is the reverse, when the primary system reassumes processing. The FDIC's contingency plan test performed both actions to determine whether its backup processing site is able to adequately assume its responsibilities in the event of a real emergency.

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Appendix II – Objective, Scope, and Methodology

The objective of this performance audit was to assess the effectiveness of controls for securing and managing the Windows Active Directory to protect the FDIC's network, systems, and data. Cotton conducted the audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) (2018 revision).[32] These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We assessed the effectiveness of internal controls that we deemed significant to the audit objective. Specifically, we assessed 12 of the 17 internal control principles defined in GAO's *Standards for Internal Control in the Federal Government* (the Green Book) (September 2014).[33] **Table 7** below summarizes the principles we assessed.

Table 7: Internal Control Principles Assessed

Control Environment
Principle 2 – Exercise Oversight Responsibility
Principle 3 – Establish Structure, Responsibility, and Authority
Principle 4 – Demonstrate Commitment to Competence
Principle 5 – Enforce Accountability
Risk Assessment
Principle 6 – Define Objectives and Risk Tolerances
Principle 7 – Identify, Analyze, and Respond to Risks
Control Activities
Principle 10 – Design Control Activities
Principle 11 – Design of Activities for the Information System
Principle 12 – Implement Control Activities
Information and Communication
Principle 14 – Communicate Internally
Monitoring
Principle 16 – Perform Monitoring
Principle 17 – Evaluate Issues and Remediate Deficiencies

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

The report presents the internal control deficiencies we identified. Because our audit was limited to the 12 principles presented above, it may not have disclosed certain internal control deficiencies that may have existed at the time of the audit.

We assessed the effectiveness of the FDIC's AD implementation in 12 security control areas covered by NIST Special Publications and Microsoft best practices. See **Table 8** below for the control areas.

[32] Cotton began this performance audit in September 2020. The 2018 revision of GAGAS became effective for performance audits beginning on or after July 1, 2019.

[33] The Green Book organizes internal control through a hierarchical structure of 5 components and 17 principles. The five components, which represent the highest level of the hierarchy, consist of the Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring. The 17 principles support the effective design, implementation, and operation of the components, and represent the requirements for establishing an effective internal control system.

Table 8: Description of Assessed Controls

Selected AD Control Areas	Definition
1. **AD Policies and Procedures**: The FDIC accurately documents the structure of its AD implementation and administrative maintenance activities.	NIST SP 800-53 Rev. 4 Control AC-1, *Policy and Procedures*, requires agencies to develop and document access control policies and procedures to address purpose, scope, roles, and responsibilities. Additionally, the policies and procedures should be updated at a defined frequency and after key events.
2. **Account Configuration**: Key accounts (objects) are configured with attributes that adhere to least privilege.	According to the Microsoft Document AD Domain Services Design Requirements, prior to the deployment of AD, the agency must plan for and design the AD logical structure. This includes determining the number of forests the agency requires, then creating designs for domains, DNS infrastructure, and organizational units. NIST SP 800-53 Rev. 4 Control AC-6, *Least Privilege*, requires agencies to employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks.
3. **Audit Logging and Monitoring**: The FDIC generates and reviews audit logs related to its Windows infrastructure, including AD, for indications of inappropriate or unusual activity.	NIST SP 800-92, *Guide to Computer Security Log Management* (September 2006), recommends that agencies review and analyze audit records (logs) for indications of inappropriate or unusual activity. An audit log is a record of events occurring within an information system or network.
4. **Configuration Management**: The FDIC maintains a secure configuration for the software that makes up the Windows infrastructure.	NIST SP 800-128, *Guide for Security-Focused Configuration Management*, states that Common Secure Configurations identify commonly recognized and standardized secure configurations to be applied to configuration items. Agencies may have deviations from the baseline due to mission requirements or other constraints. However, they must be controlled through approvals, justifications, and compensating controls.
5. **Contingency Planning**: The FDIC develops and tests a contingency plan to ensure that AD is able to continue operations in an emergency.	NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, states that a key component of contingency planning is developing and testing system contingency plans designed to recover and restore systems in the event of a disruption. Contingency plans help to ensure the availability of critical IT resources and continuity of operations in an emergency.
6. **Vulnerability Remediation**: The FDIC should scan its systems for vulnerabilities at a defined frequency, analyze scan reports, and remediate vulnerabilities within a defined timeframe.	NIST SP 800-53 Rev. 4 Control RA-5, *Vulnerability Monitoring and Scanning*, states that agencies should scan for vulnerabilities at a defined frequency, analyze scan reports, and remediate vulnerabilities within a defined timeframe.
7. **Patch Management**: The FDIC timely deploys patches to remediate software vulnerabilities.	NIST SP 800-40, *Guide to Enterprise Patch Management Technologies*, defines Patch Management as the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware. From a security perspective, patches are most often of interest because they are mitigating software flaw vulnerabilities; applying patches to eliminate these vulnerabilities significantly reduces the opportunities for exploitation.
8. **Operating System Maintenance**: The Windows Operating Systems used at the FDIC are still supported by the vendor.	NIST SP 800-53 Rev. 4 Control SA-22, *Supported System Components*, states that the agency must replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.
9. **Access Management**: The FDIC defines and implements account management requirements, including defining the conditions for group membership; requiring new user	NIST SP 800-53 Rev. 4 Control AC-2, *Account Management*, defines agency account management requirements, including defining the conditions for group membership; requiring new user approvals; defining policies for

approvals; defining policies for creating, modifying, disabling, and removing accounts; and reviewing accounts for compliance with account management requirements.	creating, modifying, disabling, and removing accounts; and reviewing accounts for compliance with account management requirements.
10. **Privileged Account Management**: Privileged accounts and groups in Active Directory are those to which powerful rights, privileges, and permissions are granted that allow the privileged accounts to perform nearly any action in AD and on domain-joined systems. The FDIC ensures that access to these types of accounts is limited only to those who need them.	NIST SP 800-53, Rev. 4 Control AC-5 *Least Privilege*, states that restricting privileged accounts to specific personnel or roles prevents day-to-day users from accessing privileged information or privileged functions. Additionally, Microsoft AD DS document Appendix B: Privileged Accounts and Groups in Active Directory, states that in AD, "Privileged" accounts and groups in Active Directory are those to which powerful rights, privileges, and permissions are granted that allow them to perform nearly any action in Active Directory and on domain-joined systems.
11. **Password Management**: The FDIC ensures that its personnel create and maintain passwords that are hard to guess and comply with FDIC policies.	NIST SP 800-53 Rev. 4 Control IA-5, *Authenticator Management*, states that individual authenticators may include passwords, tokens, biometrics, public key infrastructure certificates, and key cards. Information systems support individual authenticator management by agency-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections.
12. **Defining Key AD Points of Contact**: The FDIC ensures that its key AD administrative roles are filled by appropriate personnel with sufficient Federal oversight.	NIST SP 800-53 Rev. 4 Control AC-2, *Account Management*, states that the agency is responsible for identifying and selecting types of information system accounts to support agency missions/business functions. Additionally, it specifies authorized users of the information system, group and role membership, and access authorizations and other attributes as required for each account.

Source: Cotton scoping of the audit.

We selected these 12 areas because a control failure in these areas could impair the FDIC's ability to ensure the confidentiality, integrity, and availability of sensitive FDIC data. Such a failure could also impair the FDIC's ability to support its business operations and communications.

We assessed the design, implementation, and operating effectiveness of selected controls within each of the 12 security control areas by:

- Assessing the extent to which FDIC policies, procedures, and guidance related to AD and access management aligned with NIST and government-wide security policy and guidance.
- Performing inquiries of CIOO personnel regarding the implementation of their responsibilities for administering AD; maintaining the AD's logical structure; and defining privileged roles.
- Selecting a sample of user accounts to assess the consistency of the FDIC's practices for provisioning accounts within AD.
- Testing the effectiveness of selected controls relevant to the confidentiality, integrity, and availability of AD, including logging and monitoring, configuration management, contingency planning, patch management, and vulnerability remediation processes.

- Obtaining access to a file that included password hashes for all users in the (b) (7)(E) domains,[34] with approval and assistance of senior FDIC IT management and CIOO engineers, and attempting to recover the original passwords from the password hashes using a sophisticated proprietary "cracking" system with the assistance of our subcontractor. Performing a series of tests on privileged accounts to determine whether there were any individual password practices that rendered them susceptible to compromise.
- Using a custom RedHat Enterprise Linux image with publicly available query tools installed to assess AD and account configurations for potential attack paths.
- Using system-generated user listings to determine the effectiveness of inactivity and user termination processes.

We used NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013),[35] as the primary criteria for determining whether the FDIC had established and implemented effective controls to secure and manage its AD. We supplemented NIST SP 800-53, Rev. 4, with other SPs including, NIST SP 800-92, *Guide to Computer Security Log Management* (September 2006); NIST SP 800-128*, Guide for Security-Focused Configuration Management* (October 2019); NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems* (November 2010); and NIST SP 800-40 Rev. 3, *Guide to Enterprise Patch Management Technologies* (July 2013). We also reviewed best practices from the Federal Information Security Modernization Act of 2014; Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* (March 2006); and Microsoft best practices detailed within Microsoft's publicly available documents.

We discussed our preliminary exceptions and conclusions with representatives of FDIC management throughout the audit. We performed the majority of our work virtually due to the COVID-19 pandemic.

[34] We began performing analysis on the file 90 days after extraction to ensure that we did not crack any passwords that were in use at that time because the FDIC employs a 90-day maximum password age.
[35] Our fieldwork was conducted using NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Information Systems and Organizations*, which was in effect at the time, but has since been updated to Rev. 5, effective September 2021.

Appendix III – List of Acronyms

Acronym	Description
AD	Active Directory
AS	Authentication Server
CIO	Chief Information Officer
CIOO	Chief Information Officer Organization
(b) (7)(E)	[redacted]
DNS	Domain Name System
FDIC	Federal Deposit Insurance Corporation
GAGAS	Generally Accepted Government Auditing Standards
IP	Internet Protocol
IT	Information Technology
KDC	Key Distribution Center
NIST	National Institute of Standards and Technology
PIV	Personal Identity Verification
(b) (7)(E)	[redacted]
QA	Quality Assurance
RBAC	Role-Based Access Control
SP	Special Publication
SPN	Service Principal Name
TGS	Ticket-Granting Server
TGT	Ticket-Granting Ticket

Part II

****

FDIC Comments and OIG Evaluation

FDIC Comments and OIG Evaluation

On February 14, 2023, the FDIC's Chief Information Officer and Chief Information Security Officer provided a written response to a draft of this report, which is presented in its entirety beginning on page II-2. In its response, the FDIC concurred with all 15 of the report's recommendations. All of the recommendations in this report will remain open until we confirm that corrective actions have been completed and actions are responsive. A summary of the FDIC's corrective actions begins on page II-9.

NONPUBLIC//FDIC INTERNAL ONLY

Federal Deposit Insurance Corporation

MEMO

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

FROM: Sylvia W. Burns
SYLVIA BURNS Digitally signed by SYLVIA BURNS Date: 2023.02.14 09:41:41 -05'00'
Chief Information Officer, Chief Privacy Officer, and Director, Division of Information Technology

Zachary N. Brown
Chief Information Security Officer
ZACHARY BROWN Digitally signed by ZACHARY BROWN Date: 2023.02.14 09:31:50 -05'00'

CC: Sanjeev Purohit, Acting Deputy CIO for Technology/Chief Technology Officer
Mark F. Mulholland, Deputy CIO for Management
E. Marshall Gentry, Chief Risk Officer

DATE: February 14, 2023

RE: Draft Audit Report, entitled FDIC's Security Controls over Microsoft Windows Active Directory

Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft audit report, entitled *FDIC's Security Controls over Microsoft Windows Active Directory (No. 2021-007)*. The OIG issued the draft report on January 25, 2023. The objective of the audit was to assess the effectiveness of controls for securing and managing the Windows Active Directory to protect the FDIC's network, systems, and data. The FDIC utilizes the Active Directory as an enterprise solution for centrally managing user identification, authentication, and authorization to network resources.

The audit found that the FDIC had effective controls in place to secure and manage the Active Directory in 5 of 12 security control areas assessed (i.e., configuration management, contingency planning, patch management, vulnerability remediation, and defining key Active Directory points of contact). The audit report also stated that the FDIC:

- Established processes to restrict privileged access to a limited set of personnel and that privileged Active Directory responsibilities were granted sparingly with oversight by the Chief Information Officer (CIO) Organization's (CIOO) Cloud, Infrastructure and Platform Services personnel.
- Developed adequate mechanisms to identify suspicious events affecting the Active Directory environment and notify appropriate personnel; reviewed alert triggers for effectiveness; and retained audit logs in accordance with retention requirements.
- Determined that network passwords reviewed during the audit complied with FDIC password length and complexity requirements and only identified limited instances of shared common root words.
- Established effective processes for provisioning and approving Domain Administrators and Wintel Administrators.

Federal Deposit Insurance Corporation

Further, the audit report noted that the FDIC's extensive use of multi-factor authentication meant that having a password alone generally will not result in obtaining access to an account.

The audit report contains 15 recommendations to address weaknesses identified in the remaining seven security control areas assessed by the OIG. FDIC management concurs with the recommendations. A summary of our planned corrective actions and associated milestones follows.

MANAGEMENT RESPONSE

Recommendation 1 –

We recommend that the CIO:

1. Provide additional training to emphasize password requirements for privileged account users and communicate the effect of poor password practices, including those identified in this report.

   Management Decision: Concur

   Corrective Action: The CIOO will review, revise, and provide privileged account user training that emphasizes password requirements and communicates the effect of poor password practices.

   Estimated Completion Date: 03/31/2024

Recommendation 2 –

We recommend that the CIO:

2. Develop and implement controls to monitor and track password usage for privileged users and domain administrators to mitigate insecure password practices.

   Management Decision: Concur

   Corrective Action: The CIOO will develop and implement policies and procedures that require privileged users and domain administrators in the Active Directory to manage passwords in the (b) (7)(E) which will automatically create and manage passwords consistent with established policies specific to administrator accounts. These policies and procedures will address expectations for the use of the (b) (7)(E)

   Estimated Completion Date: 07/31/2023

Federal Deposit Insurance Corporation

Recommendation 3 –

We recommend that the CIO:

3. Approve and maintain Secure Baseline Configuration Guide deviations for accounts in the [redacted] domain, as appropriate.

   Management Decision: Concur

   Corrective Action: The CIOO will evaluate the standard configuration requirements for Active Directory accounts in the [redacted] domain, obtain approval for any deviations, and update the Secure Baseline Configuration Guide as appropriate.

   Estimated Completion Date: 10/31/2023

Recommendation 4 –

We recommend that the CIO:

4. Develop and implement policies and procedures to automate the password creation and management process for privileged Active Directory accounts.

   Management Decision: Concur

   Corrective Action: As stated in our response to Recommendation 2, the CIOO will develop and implement policies and procedures that require privileged Active Directory accounts to be managed in the [redacted] which will automatically create and manage passwords consistent with established policies specific to administrator accounts.

   Estimated Completion Date: 11/30/2023

Recommendation 5 –

We recommend that the CIO:

5. Remove unnecessary elevated domain privileges for accounts across all FDIC domains.

   Management Decision: Concur

   Corrective Action: The CIOO will review privileges for Active Directory accounts across all FDIC domains and remove any elevated domain privileges that are determined to be unnecessary.

   Estimated Completion Date: 06/30/2023

Federal Deposit Insurance Corporation

Recommendation 6 –

We recommend that the CIO:

6. Develop and implement permission settings and configurations for privileged accounts that are aligned with the principle of least privilege.

   Management Decision: Concur

   Corrective Action: The CIOO will review and update the Role Based Access Configuration baseline for Active Directory administrator accounts to align with the principle of least privilege and ensure that any necessary changes to the baseline are implemented.

   Estimated Completion Date: 08/31/2023

Recommendation 7 –

We recommend that the CIO:

7. Develop and implement monitoring mechanisms to regularly review privileged account settings and configurations and remediate any misconfigured accounts.

   Management Decision: Concur

   Corrective Action: The CIOO will develop and implement a written procedure to regularly review privileged account settings and configurations and remediate any misconfigured accounts.

   Estimated Completion Date: 09/29/2023

Recommendation 8 –

We recommend that the CIO:

8. Identify inactive user accounts and disable or delete them in accordance with FDIC policy.

   Management Decision: Concur

   Corrective Action: The CIOO will review Active Directory accounts identified during the audit to determine if they need to be disabled or removed and take appropriate actions.

   Estimated Completion Date: 06/30/2023

Federal Deposit Insurance Corporation

Recommendation 9 –

We recommend that the CIO:

9. Design and implement mitigating controls to address occurrences where the automated inactivity setting is inoperable.

   Management Decision: Concur

   Corrective Action: The CIOO will develop a written procedure to manually disable inactive accounts in the Active Directory should the automated inactivity setting become inoperable. As an added mitigating control, the CIOO will implement a quarterly review to validate that user accounts comply with FDIC policy requirements for disabling and deleting accounts.

   Estimated Completion Date: 12/31/2023

Recommendation 10 –

We recommend that the CIO:

10. Develop and implement a process to regularly evaluate the roles to determine whether they are still needed or duplicative of other roles.

    Management Decision: Concur

    Corrective Action: The CIOO will coordinate with business Divisions and Offices to develop and implement a process for reviewing Active Directory roles and associated access to determine whether they are still needed or are duplicative of other roles, and will implement appropriate actions based on the results of the reviews. The reviews will be conducted on a frequency commensurate with risk.

    Estimated Completion Date: 03/30/2024

FDIC Federal Deposit Insurance Corporation

Recommendation 11 –

We recommend that the CIO:

11. Develop and implement a process to reconcile conflicting certification determinations for duplicative roles.

    Management Decision: Concur

    Corrective Action: The FDIC has a business need to maintain separate roles that have similar, but not duplicative, permissions. We expect that the corrective actions taken in response to Recommendation 10, which include the removal of duplicative roles, will substantially mitigate the risk of conflicting certification determinations. We will assess the effectiveness of the actions taken in response to Recommendation 10 to confirm that they mitigate the risk of conflicting certifications and, if warranted, will take additional steps to further mitigate the risk.

    Estimated Completion Date: 03/30/2024

Recommendation 12 –

We recommend that the CIO:

12. Update and implement procedures to proactively update or replace operating systems before vendor support ends.

    Management Decision: Concur

    Corrective Action: The CIOO's Infrastructure and Operations Services Branch, working in coordination with the Enterprise Strategy Branch, will document and implement procedures to monitor for vendor end-of-life support for operating systems and take appropriate action to upgrade or replace affected systems. Any exceptions will require a documented justification and management approval.

    Estimated Completion Date: 12/30/2023

Federal Deposit Insurance Corporation

Recommendation 13 –

We recommend that the CIO:

13. Issue a current, updated Active Directory Operations Manual.

    Management Decision: Concur

    Corrective Action: The CIOO will update and reissue the Active Directory Operations Manual as part of the Windows 2019 Migration Project.

    Estimated Completion Date: 06/30/2023

Recommendation 14 –

We recommend that the CIO:

14. Develop and implement procedures to regularly update the Active Directory Operations Manual to reflect the current structure and practices.

    Management Decision: Concur

    Corrective Action: The CIOO will include the Active Directory Operations Manual in the managed document review and update process handled by the FDIC's enterprise information technology service management platform—ServiceNow. As such, the manual's owner will receive periodic reminders to review and update the document.

    Estimated Completion Date: 06/30/2023

Recommendation 15 –

We recommend that the CIO:

15. Develop and implement a process to monitor all domain controllers and ensure that any exceptions are addressed timely.

    Management Decision: Concur

    Corrective Action: The CIOO will revise the Windows Operations Manual to require the use of a standard build template for domain controllers to ensure automated performance monitoring is enabled and integrated with the Active Directory policy. In addition, the CIOO will revise the Windows Operations Manual to define procedures for monitoring domain controllers to ensure they remain in compliance with approved configurations and that any exceptions are addressed in a timely manner.

    Estimated Completion Date: 07/31/2023

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 review, revise, and provide privileged account user training that emphasizes password requirements and communicates the effect of poor password practices.	March 31, 2024	$0	Yes	Open
2	The CIOO will develop and implement policies and procedures that require privileged users and domain administrators in the Active Directory to manage passwords in the (b) (7)(E) , which will automatically create and manage passwords consistent with established policies specific to administrator accounts. These policies and procedures will address expectations for the use of the (b) (7)(E) .	July 31, 2023	$0	Yes	Open
3	The CIOO will evaluate the standard configuration requirements for Active Directory accounts, obtain approval for any deviations, and update the Secure Baseline Configuration Guide as appropriate.	October 31, 2023	$0	Yes	Open
4	The CIOO will develop and implement policies and procedures that require privileged Active Directory accounts to be managed in the (b) (7)(E) , which will automatically create and manage passwords consistent with established policies specific to administrator accounts.	November 30, 2023	$0	Yes	Open
5	The CIOO will review privileges for Active Directory accounts across all FDIC domains and remove any elevated domain privileges that are determined to be unnecessary.	June 30, 2023	$0	Yes	Open

6	The CIOO will review and update the Role Based Access Configuration baseline for Active Directory administrator accounts to align with the principle of least privilege and ensure that any necessary changes to the baseline are implemented.	August 31, 2023	$0	Yes	Open
7	The CIOO will develop and implement a written procedure to regularly review privileged account settings and configurations and remediate any misconfigured accounts.	September 29, 2023	$0	Yes	Open
8	The CIOO will review Active Directory accounts identified during the audit to determine if they need to be disabled or removed and take appropriate actions.	June 30, 2023	$0	Yes	Open
9	The CIOO will develop a written procedure to manually disable inactive accounts in the Active Directory should the automated inactivity setting become inoperable. As an added mitigating control, the CIOO will implement a quarterly review to validate that user accounts comply with FDIC policy requirements for disabling and deleting accounts.	December 31, 2023	$0	Yes	Open
10	The CIOO will coordinate with business Divisions and Offices to develop and implement a process for reviewing Active Directory roles and associated access to determine whether they are still needed or are duplicative of other roles, and will implement appropriate actions based on the results of the reviews. The reviews will be conducted on a frequency commensurate with risk.	March 30, 2024	$0	Yes	Open
11	The FDIC has a business need to maintain separate roles that have similar, but not duplicative, permissions. The FDIC expects that the corrective actions taken in response to Recommendation 10, which include the removal of duplicative roles, will substantially mitigate the risk of conflicting certification determinations. The FDIC will assess the effectiveness of the actions taken in response to Recommendation 10 to confirm that they mitigate the risk of conflicting certifications and, if warranted, will take additional steps to further mitigate the risk.	March 30, 2024	$0	Yes	Open

12	The CIOO's Infrastructure and Operations Services Branch, working in coordination with the Enterprise Strategy Branch, will document and implement procedures to monitor for vendor end-of-life support for operating systems and take appropriate action to upgrade or replace affected systems. Any exceptions will require a documented justification and management approval.	December 30, 2023	$0	Yes	Open
13	The CIOO will update and reissue the Active Directory Operations Manual as part of the Windows 2019 Migration Project.	June 30, 2023	$0	Yes	Open
14	The CIOO will include the Active Directory Operations Manual in the managed document review and update process handled by the FDIC's enterprise information technology service management platform. As such, the manual's owner will receive periodic reminders to review and update the document.	June 30, 2023	$0	Yes	Open
15	The CIOO will revise the Windows Operations Manual to require the use of a standard build template for domain controllers to ensure automated performance monitoring is enabled and integrated with the Active Directory policy. In addition, the CIOO will revise the Windows Operations Manual to define procedures for monitoring domain controllers to ensure they remain in compliance with approved configurations and that any exceptions are addressed in a timely manner.	July 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.