Background Investigations for Privileged Account Holders

June 2022 **AEC Memorandum 22-002**

Memorandum

Audits, Evaluations, and Cyber

☆☆☆☆☆☆☆☆

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

Date: June 22, 2022

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

Daniel H. Bendler
Deputy to the Chairman and Chief Operating Officer

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

Subject: **Management Advisory Memorandum |** Background Investigations for Privileged Account Holders | AEC Memorandum 22-002

During the course of our ongoing audit of security controls over the Federal Deposit Insurance Corporation's (FDIC) Windows Active Directory, we identified concerns warranting urgent attention.[1] We found that the FDIC does not have adequate controls to ensure that certain contractors and employees who require privileged access to FDIC information systems and data have background investigations (BI) commensurate with appropriate determinations of risk.

Background

The Office of Management and Budget Circular A-130 requires that agencies implement access control policies for information resources that ensure individuals have the appropriate background investigation conducted prior to granting access.

The FDIC's Personnel Security and Suitability Program (PSSP) is designed to ensure that its employees and contractor personnel (contractors) meet applicable Federal security and suitability requirements allowing for the successful execution of the FDIC's mission. The effectiveness of the FDIC's PSSP is important to ensure that FDIC employees and contractors are properly screened and investigated before being granted access to information systems and entrusted with sensitive or confidential information.

[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 include independence, analysis, evidence review, indexing and referencing, legal review, and supervision. See also, the Pandemic Response Accountability Committee Agile Products Toolkit https://www.pandemicoversight.gov/media/file/agile-products-toolkit0pdf.

Employee Background Investigations

To support the PSSP, the FDIC Directive 2120.1, *Personnel Security and Suitability Program for Applicants and Employees*, requires that each FDIC position be evaluated and assigned a risk designation commensurate with the position's duties and responsibilities. Based on this risk designation, the FDIC must conduct an appropriate BI. This Directive also requires that Information Security Managers (ISM) within FDIC Divisions and Offices ensure that the assigned risk designation is consistent with the position's access to information technology (IT) systems and data.[2] To assign the appropriate risk designation level, the ISM utilizes the Position Designation Tool compiled by the Office of Personnel Management (OPM).

The FDIC's Personnel Security Guide for Employee Background Investigations describes three risk levels for IT-related positions (low, moderate, and high) and related impacts. A "high risk" level has the potential for exceptionally serious impact involving duties especially critical to the FDIC's mission, with broad scope and authority and with major program responsibilities that affect a major computer/automated data processing (ADP) system(s). A "moderate risk" has the potential for moderate to serious impact involving duties of considerable importance to the FDIC's mission with significant program responsibilities that affect large portions of a computer/ADP system(s). A "low risk" has the potential for impact involving duties of limited relation to the FDIC's mission through the use of a computer/ADP system(s).

Contractor Background Investigations

The FDIC Directive 1610.02, *Personnel Security and Suitability Program for Contractors and Contractor Personnel*, requires that all contractors be subject to a BI commensurate with the risk designation for the position.[3] According to FDIC Directive 1610.02, the FDIC assigns contractors to one or more labor categories or areas of functional responsibility with an assigned risk designation level(s). When a contractor performs in more than one labor category or area of functional responsibility and the assigned risk designation levels are not the same, the FDIC applies the highest risk designation level to the individual.

Program Managers and Oversight Managers are responsible for determining the risk designations related to contractor labor categories and areas of functional responsibility. ISMs and the FDIC's SEPS review and approve these risk designations.[4] The FDIC's SEPS

---

[2] FDIC Form 1600/11, *Position Designation Record*, is completed and signed by a manager/supervisor. ISMs then review the risk designation level, and the Security and Emergency Preparedness Section (SEPS) conducts a review to approve or reject the risk designation for each position.
[3] The FDIC has established low, moderate, and high risk designation criteria for contractors similar to that of its employees. FDIC Directive 1610.02 provides details regarding the risk designation levels for contractors associated with various functional responsibilities.
[4] FDIC Form 1600/17, *Contractor Risk Level Record*, is completed and signed by a Program Manager or Oversight Manager. The ISMs then conduct a risk level review and either concur or adjust the risk designation. SEPS conducts a review to approve or reject the risk designation for each position.

Personnel Security Procedures Guide for Contract Officers and Oversight Managers provides further guidance for assessing risk designations associated with contractors.

Privileged Accounts

The FDIC assigns privileged accounts to employees and contractors to administer IT resources, such as workstations, servers, and the FDIC's Active Directory. A privileged account holder may have access and authority to control and monitor systems, and perform administrative functions that ordinary users are not authorized to perform.[5] For example, a privileged user may have the ability to modify, delete, or change data, and may have the ability to change configuration settings on servers that contain sensitive FDIC data. The FDIC does not require a "high risk" designation level for all privileged account holders.

Results of Work Performed to Examine BIs for Privileged Account Holders

During the course of our ongoing audit of the FDIC's Active Directory, we reviewed 144 privileged account holders to determine whether the FDIC conducted BIs commensurate with the position risk designation levels (low risk, moderate risk, or high risk) recorded in the FDIC's personnel system, Corporate Human Resources Information System (CHRIS); and whether the BIs for these privileged account holders were favorably adjudicated and if not, whether their privileged access was removed in a timely manner.[6] We found that:

- BIs initiated and/or completed by the FDIC matched the information in the FDIC's personnel system with one exception. For one privileged account holder, the FDIC had not conducted a BI commensurate with the risk designation level in CHRIS. We notified the FDIC that the employee had a moderate BI that did not match the high risk designation level in CHRIS. In response, the FDIC informed the OIG that this employee had the appropriate BI level for their privileged access. Upon further inquiry, however, we learned the employee did not have the appropriate BI for their assigned position. Specifically, the employee was hired as an IT Specialist in June 2020 and placed on a position description (PD) with a moderate risk designation. On February 28, 2021, the FDIC reassigned the employee to a PD with a high risk designation. However, the FDIC did not properly initiate the required upgrade to the employee's BI from a moderate to high until October 2021. The FDIC had originally initiated the upgrade in March 2021, but due to an administrative error on the associated forms, the upgraded BI was

[5] The Cybersecurity Act defines a privileged user as "a user who has access to system control, monitoring, or administrative functions." Cybersecurity Act § 406 (a)(5).
[6] In January 2021, we issued an OIG evaluation report on *The FDIC's Personnel Security and Suitability Program*. We determined that the FDIC's PSSP was not fully effective in ensuring that: (1) preliminary background investigations were completed in a timely manner; (2) background investigations were ordered and adjudicated commensurate with position risk designations; and (3) re-investigations were ordered within required timeframes. This evaluation did not review BIs specific to privileged account holders.

processed at the same moderate risk level and closed.[7] In October 2021, the FDIC questioned the discrepancy between the employee's BI and risk designation level and took action with a new request for an upgraded BI. The FDIC favorably adjudicated the employee on June 1, 2022.[8] The employee had privileged access to FDIC's systems and data for approximately 15 months (February 28, 2021- June 1, 2022) between the time the FDIC assigned the employee to a PD with a high risk designation and favorably adjudicated the BI.

- Privileged account holders were favorably adjudicated with one exception. Specifically, we found that the FDIC had conducted a preliminary BI for a contract employee in February 2021 and granted access to a privileged account in April 2021. However, the BI was not adjudicated until November 2021, and the adjudication was unfavorable at that time. Based on the adjudication, the FDIC ceased the privileged access and terminated the contractor consistent with its policies and procedures. The contractor had access to privileged accounts for approximately 7 months while the BI was being adjudicated.

Concerns Related to Ensuring Appropriate BIs for Privileged Account Holders

During our review, we also noticed that of the 144 privileged account holders, the FDIC had assigned a "high" risk designation for 132 account holders (92 percent) and had, therefore, conducted a "high" BI for these individuals. For the other 12 privileged account holders consisting of both contractors and employees, the FDIC did not conduct a "high" BI.

- For 9 of the 12 privileged account holders, the FDIC determined that the risk designation for the positions held by these individuals was "low" or "moderate," which eliminated the need for a "high" BI.[9] We did not examine the supporting documentation for the FDIC's risk designation determinations; however, it was not clear whether the FDIC had processes in place to consider the privileged access of these individuals in their original risk designations or re-evaluate their risk designations when their access changed. We reviewed the PDs for five of the nine privileged account holders that were FDIC employees and found that the PDs did not clearly indicate a need for privileged access to information systems and data. Therefore, it is not clear whether this information was considered as part of the procedures for evaluating risk designations through the PD process. Further, the PD process may not need to reflect the privileged access since all individuals assigned to a PD may not require privileged access to information systems and data.

[7] As a result of an OIG evaluation of the FDIC's PSSP, in January 2021, FDIC Divisions and Offices began to review and validate the risk level designations on employee PDs and ensure that appropriate BIs were performed.
[8] During this timeframe, the employee submitted paperwork for the background investigation and the investigation was conducted and adjudicated.
[9] For the remaining three privileged account holders, the position risk designations in CHRIS were "high" but the FDIC did not complete the corresponding BI for various reasons.

Based on further inquiry, we found that the FDIC does not have policies or procedures in place to re-evaluate the risk designations and BI levels for FDIC employees or contractors who transition from being non-privileged account holders to privileged account holders or whose privileged access is increased after they have already started work at the FDIC. Such controls can help ensure that the FDIC considers the risks resulting from a contractor or employee's change in privileged access and that the appropriate BI level is in place before granting the privileged access. Such controls are also consistent with OMB A-130, which requires that "individuals have appropriate authorization and need, *and that the appropriate background investigation is conducted* (emphasis added) prior to granting access."

Additionally, the FDIC's existing BI and information system access controls do not fully mitigate risks in this area. For example, the FDIC may not be aware of the future need for privileged account access at the time a contractor or employee is hired and the risk designation level is determined. An individual may also change job responsibilities and require privileged access that was not originally anticipated or considered in the risk designation level for the position. In addition, the FDIC has not incorporated controls within its Access Request and Certification System (ARCS) to require that the Agency re-evaluate the risk designation and BI level for contractors and employees who transition from non-privileged account holders to privileged ones or whose privileged access is increased.

Thus, the FDIC cannot be sure that certain employees and contractors who are granted privileged access to the FDIC's information systems and related data in the future will have an appropriate risk designation level and related BI. Without proper controls, the FDIC incurs greater risk of unauthorized access to its data and information systems.

FDIC Response

The FDIC's Chief Information Officer and Chief Operating Officer provided a written response, dated June 16, 2022, to a draft of this memorandum addressing the OIG's concerns. The FDIC agreed that procedures could be improved in this area and plans to perform follow-up work to further assess the extent of risk associated with the OIG's observations and make improvements to procedures and processes as warranted by the end of this calendar year. The response is presented in its entirety in the Appendix.

Federal Deposit Insurance Corporation

Memorandum

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

FROM: Sylvia W. Burns SYLVIA BURNS Digitally signed by SYLVIA BURNS Date: 2022.06.16 12:28:47 -04'00'
Chief Information Officer, Chief Privacy Officer, and Director, Division of Information Technology

Daniel H. Bendler DANIEL BENDLER Digitally signed by DANIEL BENDLER Date: 2022.06.16 12:20:56 -04'00'
Deputy to the Chairman and Chief Operating Officer

DATE: June 16, 2022

RE: Management Advisory Memorandum | Background Investigations for Privileged Account Holders
| No. 2021-007

Thank you for the opportunity to provide a written response to the Office of Inspector General's (OIG) Management Advisory Memorandum, dated June 13, 2022, addressing FDIC background investigations (BI) for privileged account holders (Advisory Memo). The FDIC recognizes the importance of having an effective program for ensuring that FDIC employees and contractors are properly screened and investigated before being granted access to information systems and entrusted with sensitive or confidential information.

OIG-Identified Exceptions to Adequacy of Background Investigations

As described in the Advisory Memo, the OIG reviewed 144 privileged account holders to determine whether their BIs were conducted commensurate with position risk designation levels in the Corporate Human Resources Information System (CHRIS) and whether the BIs were favorably adjudicated, and if not, whether their privileged access was removed in a timely manner. The OIG found (1) an employee whose BI was not commensurate with his or her risk designation level and (2) a contractor with privileged access until their BI was unfavorably adjudicated.

With respect to the employee case, we acknowledge that the process could have been better executed. Within the context of the memorandum focusing on privileged users, we note that the change in risk designation associated with the employee was not related to newly-granted privileged access. Rather, the change was due to the FDIC assigning the employee to a new Position Description that had a high risk designation.

As it relates to the contractor, at the FDIC and many civilian agencies, there is no difference in access granted following a favorably adjudicated Full BI and Preliminary BI (PBI). This practice speeds up onboarding and ramp up time for projects and operations, thereby reducing costs and increasing delivery speed. Notably, the FDIC PBI process includes key security checks including fingerprints for

criminal history, legal/ethics checks, credit checks, and related requirements. These process elements meaningfully reduce the risk of the FDIC hiring or engaging with a potentially malicious actor.

In addition, the FDIC has several risk mitigations in place to protect IT resources during the period employees and contractors have access to IT systems and data prior to a favorably adjudicated BI. For example:

- Consistent with National Institute of Standards and Technology (NIST) guidance and FDIC Circular 1360.9, *Protecting Sensitive Information*, FDIC exercises the principle of least privilege by limiting user access permissions to FDIC systems and IT resources only to what is needed for users to complete their job functions. This approach reduces the risk associated with access (including privileged access) to FDIC systems and IT resources.
- Consistent with NIST guidance, the FDIC monitors privileged access accounts. All system administrator's access and activities are logged by the respective system and an enterprise logging tool. Questionable activity and/or concerns are referred to the Insider Threat Program for mitigation or action.
- The FDIC has a process to remove network access when an employee or contractor is terminated. As detailed in the Advisory Memo, the FDIC terminated privileged access and terminated the contractor's support of the FDIC, consistent with the Corporation's policies and procedures.

High BI Not Conducted for All Privileged Account Holders

The Advisory Memo notes that the risk designation level for the positions held by nine privileged account holders was "low" or "moderate." Therefore, the FDIC did not conduct "high" BIs for these account holders. The Advisory Memo also notes that the FDIC does not require a "high" risk designation level for all privileged account holders.

There are a number of factors that go into the risk level determination (including magnitude and scope of potential harm inflicted), and therefore, having privileged access does not by itself indicate that a "high" risk designation and high BI is warranted. Other factors include, but are not limited to, access to personal, private, controlled, unclassified, or proprietary information; the potential impact of the position on the efficiency or integrity of the service; and adjustments made based on the program designation and level of supervision.

We reviewed our records and confirmed that the risk designations for those nine privileged account holders are appropriate.

Guidance for Re-evaluating Risk Designation Levels when Transitioning From Non-Privileged to Privileged Account Holders

The OIG noted that the FDIC did not have policies, procedures, or a requirement within the Access Request and Certification System (ARCS), to re-evaluate risk designation levels for employees or contractors who transition from being non-privileged account holders to privileged account holders, or whose privileged access is increased after they start work at the FDIC. We note that the OIG did not identify any cases where the risk designation level associated with an employee or contractor should have been updated due to the addition of privileged access. Nevertheless, we concur that our procedures could be improved in this area.

Planned Steps to Address the OIG's Concerns

The FDIC recognizes that without proper controls, there is a greater risk of unauthorized access to FDIC's data and information systems. In the case of privileged users, that risk is magnified by the extent and nature of those users' responsibilities and access to systems, data, and functions. Accordingly, we plan to perform follow-up work to further assess the extent of risk associated with the OIG's observations and make improvements to procedures and processes as warranted. We expect to complete this work by the end of this calendar year. Specific timelines will be based on the level and complexity of the analysis required.

CC: E. Marshall Gentry, Chief Risk Officer and Director, Office of Risk Management and Internal Controls

Mark F. Mulholland, Deputy Chief Information Officer for Management

Montrice G. Yakimov, Chief, IT Risk, Governance, and Policy

3

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.