FDIC Office of Inspector General

The FDIC's Incident Detection and Response Program

Office of Audits

August 2026 | AUD-26-03

Office of Inspector General

REDACTED VERSION
PUBLICLY AVAILABLE

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

Integrity • Objectivity • Independence • Excellence • Transparency

☆☆☆☆☆☆☆☆

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.

Executive Summary

The FDIC's Incident Detection and Response Program (AUD-26-03) August 31, 2026

What We Did

Under Federal law and regulation, the FDIC is responsible for safeguarding information, data, and assets from loss, theft, or compromise. To accomplish this, the FDIC must maintain the ability to prepare for, respond to, and resolve computer security incidents. The objective of our audit was to determine to what extent the FDIC has implemented processes to detect, respond, and actively defend against cyber threats.

Impact on the FDIC

The Cybersecurity Infrastructure Security Agency has continued to identify cyber threats targeting critical infrastructure, such as the Financial Services Sector. Failure to protect bank, employee, and other sensitive information could cause irreparable financial, reputational, operational, or other harm to the FDIC, individuals, and entities.

What We Found

We found that the FDIC has implemented controls and processes in eight security areas to detect, respond, and actively defend against cyber threats. However, we identified improvement opportunities in three security areas covering its incident detection and response program.

Specifically, the FDIC can (1) strengthen its monitoring of endpoint detection and response logs to better detect known adversarial techniques such as running malicious code, maintaining access, and avoiding detection; (2) update its policies for involuntarily separated employees to address the elevated risk present when an employee is involuntarily separated; and (3) better align its incident response capabilities testing to National Institute of Standards and Technology (NIST) standards while improving coordination between the Office of the Chief Information Security Officer and the Division of Information Technology.

Prompt remediation of these issues will better position the FDIC to monitor, detect, and respond to threat actors in a timely manner to minimize the damage they can cause and reduce the risk to the FDIC's mission to maintain stability and public confidence in the nation's financial system.

What We Recommended

We made four recommendations to improve the FDIC's processes to detect, respond, and actively defend against cyber threats. We recommended that the FDIC assess the current process for maintaining incident detection strategies to identify where gaps in coverage exist; inspect current access permissions on FDIC endpoints and update accordingly; update applicable FDIC directives related to involuntary separations for the timely removal of logical access based on risk-driven timetables; and align current incident response testing procedures to NIST Cybersecurity Framework incident response functions. The FDIC concurred with all four recommendations and plans to complete all corrective actions by July 31, 2027.

Table of Contents

The FDIC's Incident Detection and Response Program

OBJECTIVE

The objective of our audit was to determine to what extent the Federal Deposit Insurance Corporation (FDIC) had implemented processes to detect, respond, and actively defend against cyber threats. We conducted this performance audit from April 2025 through July 2026 in accordance with the Government Accountability Office's (GAO) Generally Accepted Government Auditing Standards. 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Appendix 1 of this report includes additional details about our objective, scope, and methodology.

BACKGROUND

Under Federal law, regulation, and guidance,[1] the FDIC is responsible for safeguarding information, data, and assets from loss, theft, or compromise. To do this, the FDIC must maintain the ability to prepare for, respond to, and resolve computer security incidents,[2] hereinafter referred to as "incident(s)". Failure to protect bank, employee, and other sensitive information (e.g., facts, data, or opinions in any medium or form) could cause irreparable financial, reputational, operational, or other harm to the FDIC, individuals, and entities.

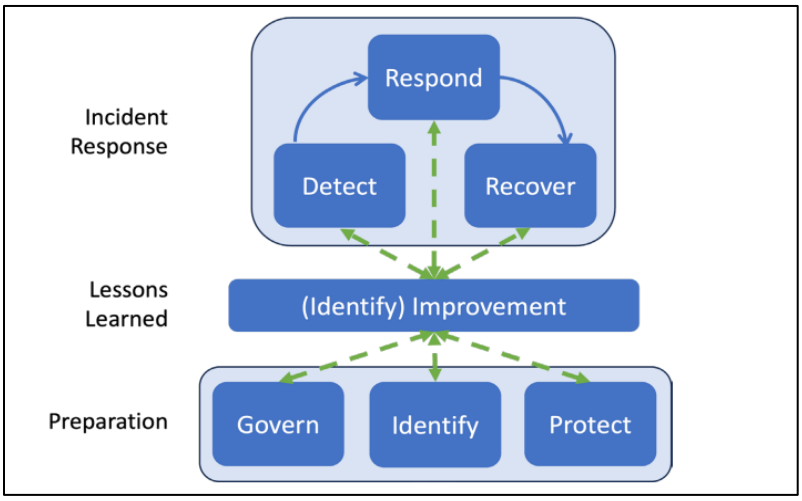
In 2024, the FDIC reported over 120 incidents[3] to the Cybersecurity Infrastructure Security Agency (CISA).[4] All incidents were scored[5] as low or negligible and unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. According to the FDIC, none of these incidents were attributed to an advanced persistent threat, nation state actor, or other threat actors. CISA has continued to identify cyber threats targeting critical infrastructure, such as the Financial Services Sector, and that nation-state actors and sponsored entities pose an elevated threat to our national security.

---

[1] See **Appendix 1**, describing our review of relevant Federal laws, regulations, and guidance.
[2] As defined in NIST Special Publication 800-61 Revision 3 – An occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
[3] As defined in the Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. No. 113-283, 128 Stat. 3073, Dec. 18, 2014, codified at 44 U.S.C. § 3552(b)(2), an incident refers to an occurrence that: (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
[4] CISA Security Incidents are comprised of Computer Security Incidents that meet the incident notification requirements outlined in the Federal Incident Notification Guidelines.
[5] Scored under the CISA National Cyber Incident Scoring System, which is used by Federal agencies to provide a repeatable and consistent mechanism for estimating the risk of an incident.

The Federal Government's approach to incident response is driven by the National Institute of Standards and Technology's (NIST) *Incident Response Recommendations and Considerations for Cybersecurity Risk Management, Special Publication* (SP) 800-61, Revision 3. The publication assists organizations with incorporating cybersecurity incident response recommendations. In addition, the publication gives organizations' considerations throughout their cybersecurity risk management activities. It also depicts the incident response lifecycle with a clear emphasis on continuous improvement across the NIST Cybersecurity Framework 2.0 Functions - Govern, Identify, Protect, Detect, Respond, and Recover. **Figure 1** depicts the relationship between preparation and improvement in the Incident Response Life Cycle.

Figure 1: Incident Response Life Cycle Model



Source: NIST SP 800-61, Rev 3, *Incident Response Recommendations and Considerations for Cyber Risk Management* (April 2025)

The FDIC's Incident Response Plan

The FDIC developed the Incident Response Plan (IRP) as a roadmap for implementing its incident response program, which also provides guidance on how to respond to incidents. The IRP defines key terms, identifies roles and responsibilities, and provides detailed information about what must happen when there is a major security incident.[6]

[6] A major incident is any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

The FDIC uses a severity classification framework[7] for incidents to ensure consistent prioritization and escalation.

Not all events result in an incident, and the FDIC's response will vary based on the potential severity of an event.[8] The IRP defines an event as any observable occurrence that may trigger tasks and notifications in the FDIC's incident response process. An incident is defined as an occurrence that: (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

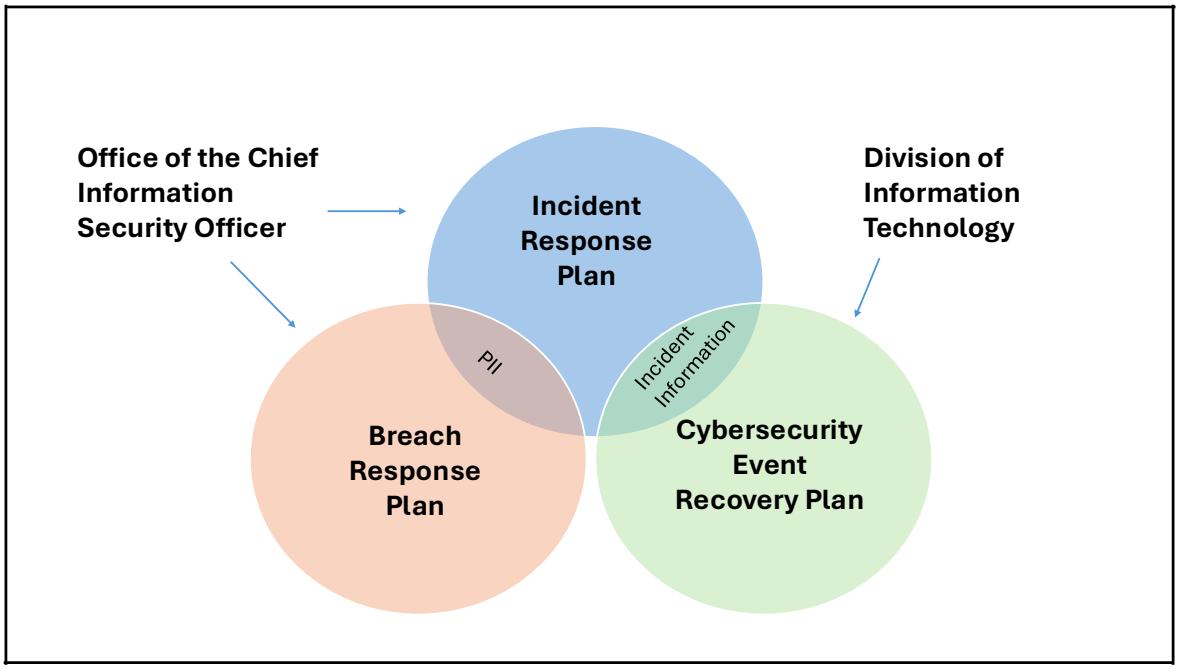
In response to an incident, the FDIC can activate other organizational plans that overlap with the IRP, such as the:

- Breach Response Plan (BRP): The purpose of the BRP is to describe the activities the FDIC takes to respond to a breach of personally identifiable information (PII); or
- Cybersecurity Event Recovery Plan (CSER): The purpose of the CSER is to assist in prevention and recovery from potential cybersecurity events.

The scope of the IRP and CSER overlap during the recovery phase of the incident response lifecycle. During this phase, the Office of the Chief Information Security Officer (OCISO) provides incident-related information and details (e.g., description of the incident, the severity, and location) to assist with Division of Information Technology (DIT) system recovery efforts, if necessary. **Figure 2** shows the relationships between the IRP, BRP, and CSER; the triggering event factors (i.e., PII and Incident Information); and the FDIC functional area responsible for executing each plan.

[7] The FDIC's Severity Classification Framework is defined by the following five categories: P-1: Critical; P-2: Severe; P-3: Elevated; P-4: Routine; P-5: Informational and is intended to be flexible to account for the many variables associated with a computer security incident.
[8] Depending on the nature and severity of the incident, an event may be classified as a Computer Security Incident and Breach, CISA Security Incident, or Major Incident. The definitions the FDIC uses are not mutually exclusive.

Figure 2: Relationship Between FDIC's IRP, BRP, and CSER



Source: Office of Inspector General (OIG) analysis of the FDIC's Incident Response Plan, Version 3.1, dated February 29, 2024

Incident Monitoring at the FDIC

NIST SP 800-53 Revision 5, Control IR-5, *Incident Monitoring*, requires organizations to track, document, and report security incidents, and maintain records of each incident. Further, organizations are encouraged to use automated tools for tracking, data collection, and analysis to streamline the process.

The FDIC's current incident monitoring process uses several security tools. Specifically, the FDIC leverages its Endpoint Detection and Response (EDR) tool to log suspicious activity and send this information to a log repository referred to as the Security Information and Event Management (SIEM) tool. The SIEM then correlates and analyzes audit logs against prebuilt use cases. Based on the prebuilt analysis, a notable event may be triaged for manual investigation or automated response. **Table 1** describes the key types of tools we evaluated, their general purpose, and the specific software solution the FDIC used during the period of our audit.

Table 1: Key Cybersecurity Tool Types Evaluated During this Audit

Tool Type	Description	FDIC Solution
Endpoint Detection and Response (EDR)	EDR is an endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware.	(b) (7)(E)
Security Information and Event Management (SIEM)	SIEM provides centralized logging capabilities for a variety of log types.	(b) (7)(E)

Source: Definitions provided by NIST (SIEM) and (b) (7)(E) (EDR)

Note: The tools listed within the table were in place at the time of testing (September 2025).

Adversary Emulation Testing

Adversary emulation has emerged as a powerful technique that simulates real-world cyberattacks to evaluate an organization's security posture. Unlike standard penetration testing, it focuses on how tools and teams respond to attacks. Organizations use the results of emulation testing to identify defensive gaps and optimize security investments.

Open-source adversary emulation projects, such as Atomic Red Team,[9] have developed libraries of tests designed to test organizations' security controls and are mapped to the MITRE ATT&CK® matrix.[10] Specifically, adversary emulation tools, such as Invoke-AtomicRedTeam, allow security professionals to execute tests as defined by the Atomic Red Team project.[11] This type of adversary emulation testing is typically performed under an assumed breach style environment.[12]

[9] Atomic Red Team is an open-source library of tests designed to test an organization's security controls, and is designed to help security teams better understand Atomic Red Team and the related collection of free and open-source tools.
[10] The MITRE ATT&CK® framework is a globally accessible knowledge base of adversary tactics and techniques, based on real-world observations, that helps organizations understand, detect, and defend against cyber threats by mapping attacker behaviors across an attack lifecycle, providing a common language for security professionals.
[11] Invoke-AtomicRedTeam is a PowerShell module that allows an organization to test its security controls and defenses against a wide range of attack techniques.
[12] Assumed breach testing is a type of test designed to simulate what could happen if an attacker successfully bypasses an organization's perimeter defenses. This type of testing can highlight vulnerabilities in an organization's detection and response functions to provide an opportunity for remediation before they are exploited by a malicious actor.

Cyber Threat Landscape at the FDIC

The source of an incident triggering an incident response can be due to threat actors that are external (e.g., nation state actors) or internal to the organization (e.g., internal threats from employees or contractors). To address the risk of potential insider threats, it is imperative that organizations timely remove access of involuntarily separated employees based on when the employee is notified of intended separation. Due to the risk of workplace violence or other undesirable events from involuntarily separated employees, CISA published an Interagency Security Committee Guide titled, *Managing Risk of Adverse/Involuntary Employee Separations.* This guide recommends that agencies should conduct a threat assessment to evaluate the likelihood and severity of potential threats posed by a separating employee. It also provides details on when the employee's access should be removed based on several factors, including the employee's history, behavior, and motivations.

Roles and Responsibilities

The **Enterprise Security Operations Section (ESOS)** within the Chief Information Officer Organization (CIOO), under the OCISO, has responsibility for the incident response function at the FDIC. The ESOS oversees the Security Operations Center (SOC) and the Security Response Team (SRT). The SOC team is responsible for monitoring the SIEM and investigating triaged events. The SRT is responsible for handling the response and eradication of potential incidents. The SOC team shares validated incidents with the SRT. The ESOS maintains these responsibilities and capabilities as part of its core functions, for which the FDIC has contracted with a managed security services provider[13] to operate the SOC and a security and privacy professional services[14] contractor to operate the SRT functions.

The **Division of Information Technology (DIT)** has the primary responsibility for incident recovery.[15] Within DIT, the FDIC Information Technology (IT) Systems Recovery Teams have responsibility to implement procedures to facilitate and support the recovery of time-sensitive business operations.

[13] A Managed Security Service Provider is a specialized cybersecurity company that provides outsourced monitoring, management, and protection of an organization's security infrastructure through services like threat detection and security device management, allowing businesses to enhance their security posture without maintaining extensive in-house security resources.
[14] A Security and Privacy Professional Services contractor is a specialized cybersecurity company that provides outsourced proactive investigation of emerging security and privacy threats for potential impact to business functions.
[15] Incident recovery is restoring normal operations.

RESULTS

Overall, we found that the FDIC has implemented processes to detect, respond, and actively defend against cyber threats. Specifically, the FDIC implemented effective controls in eight security areas we identified as significant to our objective. However, in three separate control areas, we found the FDIC could strengthen its existing controls. See **Table 4** for the list of control areas considered significant to this audit.

1. The FDIC could strengthen its monitoring of EDR logs.
   [IR-5 Incident Monitoring] We found the FDIC's SIEM tool was configured to detect pre-defined notable events; however, it did not generate notable events ingested from EDR logs for 90 percent of our adversarial emulated tests.
2. The FDIC could improve its access control policies for involuntary separations.
   [AC-1 Policy and Procedures] In some instances, the FDIC did not remove involuntarily separated users' access or disable network accounts until after the employees' termination date.
3. The FDIC could enhance its incident response testing process.
   [IR-8 Incident Response Plan] The FDIC could not provide documentation to support updates made to the incident response plan, or other organizational plans, such as the CSER, based on the results of annual testing.

Across these three controls areas, we made four recommendations to help improve the FDIC's ability to detect, respond, and actively defend against cyber threats, which are aligned to the NIST Cybersecurity Framework core functions Respond, Protect, and Identify; respectively. Prompt remediation of these issues will better position the FDIC to monitor, detect, and respond to threat actors in a timely manner to minimize the damage they can cause and reduce the risk to the FDIC's mission to maintain stability and public confidence in the nation's financial system.

Finding 1

Opportunities to Strengthen the FDIC's Monitoring of Endpoint Detection and Response Logs

We found that the FDIC's SIEM tool was configured to detect pre-defined notable events; however, the SIEM did not generate notable events[16] from ingested EDR logs for 45 (90 percent) of our 50 adversarial emulated tests, which therefore went

[16] When a correlation search is defined and then detects pre-defined malicious activity, then the SIEM or (b) (7)(E) in this case, generates a notable event. A notable event is a stored alert with a unique ID, time, status, severity and owner.

undetected within the SIEM. All our tests were aligned to MITRE ATT&CK® Tactics and Techniques (see Appendix 2 for additional details).

NIST SP 800-53 Revision 5, Control IR-5, *Incident Monitoring*, requires organizations to track, document, and report security incidents, and maintain records of each incident. Further, organizations are required to use organization-defined automated mechanisms for tracking, data collection, and analysis to streamline the process.

The FDIC uses its SIEM to aggregate logs from its EDR and triage notable events for SOC disposition or an SRT response. These notable events are generated based on EDR alerts and pre-defined correlation searches defined by the FDIC within the content development process. However, through these detection strategies, the FDIC did not ensure adequate SIEM coverage for some of the adversarial emulated tests we performed and did not mitigate the risk of adversaries disabling or interfering with security services.

The FDIC may not detect malicious threat actor activities (b) (7)(E)

[redacted]

[17] On our test machine, we had local administrator access and configured the machine to simulate an assumed breach style testing environment. Our procedures were used to assess the detection capabilities and that the actions performed would have typically been blocked by other security tools. The FDIC stated in the rules of engagement that at the time of testing, the FDIC EDR (b) (7)(E) use case was designed to complement, rather than duplicate, the capabilities of (b) (7)(E). As such, there is minimal functional overlap between the two. When (b) (7)(E) is disabled during testing, it is expected that a significant portion of the simulated attack activity may not generate meaningful alerts or events in the SIEM (b) (7)(E).

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

During our fieldwork, we provided the results with details of our emulated tests in December 2025 to FDIC management at which time a FDIC management official stated they would have their Purple Team[18] perform this coverage gap analysis with (b) (7)(E) .

Recommendation 1:

We recommend the **Director, Division of Information Technology**, update the FDIC's content development process based on emulated tests that did not generate notable events to identify where gaps in coverage exist within incident detection strategies.

Recommendation 2:

We recommend the **Director, Division of Information Technology**, review current access permissions on FDIC endpoints and update permissions accordingly to prevent unauthorized users from disabling or interfering with endpoint detection and response services.

[18] A purple team can be defined as a collaborative group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture.

Finding 2

Opportunities to Improve Access Control Policies for Involuntarily Separated Employees

We found some instances where the FDIC did not immediately remove involuntarily separated employees' logical access to the FDIC's network.[19] We identified existing procedures for immediate account disablement[20] and found this process was followed in 10 of 12 terminations in calendar year 2025. However, when we compared involuntary separations to logical access removals[21] from the FDIC's network, we found 2 of 12 (17 percent) of the involuntary separations did not have their logical access removed or account disabled until after the employees' effective separation date.[22]

In one of the two instances, an employee was terminated and had logical access removed on May 20, 2025. However, the effective date of separation was May 16, 2025. In the other instance, a terminated employee had their logical access removed on January 27, 2025. However, the effective date of separation was January 24, 2025.

In both instances, account disablement did not occur during these periods. For these two instances identified, DIT officials stated that the effective separation date was entered into the HR system at a later date and DIT had not received disablement account notifications[23] for the terminated employees from the Labor and Employee Relations Section (LERS).[24]The FDIC was unable to provide the OIG with the reason(s) why account disablement notifications were not sent to DIT

[19] We defined involuntary separations to include any separation for cause on charges of misconduct.
[20] The administrative action of preventing a user account from being used for authentication or access, while preserving the account's data, attributes, and audit history. The account still exists, but it is placed in a non-operational state and cannot be used to log in or access systems.
[21] Revoking a user's ability to access systems, applications, or data by removing their permissions or accounts.
[22] We were unable to determine the amount of time that elapsed between the notice of separation and removal of logical access because the tracking report generated through the FDIC's (b) (7)(E) and maintained by the Division of Administration did not include a time of notification of separation to the employee. See audit scope and methodology in Appendix 1.
[23] According to DIT officials and the FDIC's Immediate Account Disablement SOP, DIT is required to have documentation of the request to disable the account from authorized users and to have authorization from FDIC Access Control Federal staff. The process should begin when a deactivation request is sent by the Labor, Employment and Administration Section (LEAS), HRO, and/or other divisions to Access Control to initiate the deactivation action and leads to the deactivation of a user's account. DIT officials stated that they would not know to deactivate an account if they never receive an account disablement notification or if the request is not received timely.
[24] At the time, LERS was responsible for handling employee misconduct reviews. After a reorganization, LERS was replaced by the Labor, Employment and Administration Section (LEAS).

and why the effective separation date was entered into the HR system at a later date. The FDIC was unable to provide the requested information in part because the employees who initiated the termination action are no longer FDIC employees. However, we confirmed that in neither instance was a security incident identified.

NIST SP 800-53 Revision 5, *Control AC-1, Policy and Procedures* requires agencies to develop, document, and disseminate access control policies and procedures that address the controls in the AC family that are implemented within systems and organizations.

CISA Interagency Security Committee Guide – *Managing Risk of Adverse/Involuntary Employee Separations* states that agencies should conduct a threat assessment to evaluate the likelihood and severity of potential threats posed by an employee. [25] The guide recommends:

- Revoking access within 18 hours for a low-risk separation, which is generally the result of the employee leaving voluntarily due to retirement or securing new employment.
- Revoking access within 4 hours for a moderate-risk separation, which can be a voluntary or involuntary separation where there is reasonable cause for concern such as performance or behavioral issues.
- Revoking access within 1 hour for a high-risk separation, which refers to the separation of an employee who is likely to pose a risk of harm to themselves or others.
- Notification to IT of the date and time of the notification of separation.

FDIC Directive 1360.15, *Access Control for Information Technology Resources*, states access to IT resources is provided for legitimate business use and only after proper authorization has been provided. Access is removed if the authorized user (1) is assigned a change in job responsibilities, (2) transfers to a different organization, or (3) no longer requires access. Additionally, the policy mentions that access is removed when an authorized user is terminated or is no longer needed, and access must be removed as early as possible, in accordance with the FDIC Security and Privacy Controls Catalog.

Within the FDIC Security and Privacy Controls Catalog, there is a timing requirement for designated personnel to notify account managers within 8 hours of personnel being terminated. The controls catalog also specifies requirements to disable accounts at the earliest possible time,

[25] CISA, *Managing Risk of Adverse/Involuntary Employee Separations--An Interagency Security Committee Guide* (2024 Edition).

and no longer than 10 business days, when the accounts are in violation of organizational policy.[26]

In our assessment of FDIC policies and procedures, we found that the FDIC did establish a standard operating procedure for handling notifications of authorizations for immediate account disablement. However, other than the catalog's 10 business days to disable accounts for all terminations, the FDIC could not provide documentation identifying policies or procedures with specific timetables for revoking access based on the increased risk associated with involuntary separations, consistent with CISA best practices.

Based on our review of involuntary separation data, the FDIC sometimes removes logical access for involuntarily separated employees after 3 calendar days from separation, as noted above. Further, under CISA's best practice, a risk assessment should drive the timing of access revocation and account disablement.

Overall, the FDIC access controls directive did not adequately address the risks associated with involuntary separations, specifically the timing of logical access removal based on risk. Immediate removal of access to sensitive information for involuntarily separated employees contributes to protecting FDIC information. Involuntary separations due to adverse or other administrative actions pose an increased risk compared to voluntary separations due to an increased risk of motivation for revenge and opportunity to use stolen data for personal gain.

FDIC Best Practice

The FDIC developed an operating procedure within its current access controls processes for employees departing the FDIC via the Deferred Resignation Program, Voluntary Early Retirement Authorization, and Voluntary Separation Incentive Payment. Although this does not address involuntary separations, this document serves as a best practice for what could be implemented across other control areas.

This includes a seven-step process for access controls and security. The process begins with notifying OCISO of separating employees, which OCISO then sends to DIT. Within 2 business hours of receiving the separating employee roster, the DIT/Infrastructure and Operations Services Branch adds users to the separating employee roster to create an Active Directory group of separating employees via the (b) (7)(E) [redacted]

[26] In 2023, our Office issued a recommendation that the FDIC implement process improvements to ensure prompt notification and removal of user network accounts on or before the user's separation date. (*The Federal Deposit Insurance Corporation's Information Security Program – 2023*, Report No: AUD-23-004). In January 2026, the FDIC submitted a recommendation closure package to the OIG for review. Given the overlapping nature of the recommendation with the scope of another on-going OIG audit, this recommendation will remain open pending the results of that audit.

Recommendation 3:

We recommend the **Assistant General Counsel, Labor, Employment, & Administration Section**, update applicable FDIC directives and procedural documents, to ensure that the Division of Information Technology is notified of involuntary separations at, or prior to, the time of notification to the employee, and coordinate with appropriate stakeholders to establish risk-driven timetables for revoking and disabling access.

Finding 3

Opportunities to Enhance the FDIC's Approach to Testing Its Incident Response Capabilities

The FDIC could not provide complete documentation to support incident response capabilities testing and plan updates. Specifically, as part of its annual testing processes, the FDIC stated that the IRP is tested as part of the BRP; however, IRP testing results could not be provided to the OIG. Although the FDIC provided documentation for testing the BRP, the results of the June 2024 tests were not used to update the BRP or any portion of the IRP, which at the time of testing, was last updated in February 2024. We also found the most recent CSER was last updated in June 2018.

According to NIST SP 800-53, Revision 5, Control IR-3, *Incident Response Testing*, includes requirements to coordinate incident response testing with organizational elements responsible for related plans.[27] Further, Control IR-8, *Incident Response Plan*, states organizations are required to update the incident response plan to address problems encountered during plan testing.

Under NIST SP 800-61, Revision 3, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A Cybersecurity Framework 2.0 Community Profile*, the incident response life cycle model includes six functions: govern, identify, protect, detect, respond, and recover, as pictured in the Background at **Figure 1**. NIST Cybersecurity Framework Element ID.IM-04 states that incident response plans and other cybersecurity plans that affect operations should be maintained and improved. In addition, NIST guidance states that agencies should synchronize business continuity plans with incident response plans since incidents can undermine business resilience.

The FDIC's IRP clearly defined that the scope of the plan overlaps with other related plans, such as during the recovery phase of the incident response lifecycle. During this phase, OCISO provides incident-related information (e.g., description of the incident, the severity, and location) to help inform DIT system recovery efforts, if necessary. However, as part of its annual testing exercise and updates to the IRP, DIT and OCISO did not update the plans related to cybersecurity event recovery activities.

[27] According to *NIST SP 800-53, Revision 5, Control IR-3,* organizational plans related to incident response testing include business continuity plans, disaster recovery plans, continuity of operations plans, contingency plans, crisis communications plans, critical infrastructure plans, and occupant emergency plans.

These issues occurred because OCISO and DIT's testing processes were not aligned to test the entire NIST incident response lifecycle model, to include from incident detection through recovery, as shown in Figure 1. Further, this issue occurred because OCISO and DIT did not coordinate to ensure the IRP or other organizational plans (e.g., the CSER) were updated based on the results of incident response capabilities tests.

Untested IRPs could hinder the FDIC's ability to respond appropriately to current threats, potentially leading to prolonged, chaotic, and costly recovery efforts to mission critical and mission essential systems and functions. Without up-to-date protocols, the FDIC could also experience longer recovery times, affording attackers more time to cause harm to FDIC systems and data and disrupt operations supporting the FDIC's mission to maintain stability and public confidence in the nation's financial system.

Recommendation 4:

We recommend the **Director, Division of Information Technology**, update the current incident response testing procedures to ensure that the testing covers all National Institute of Standards and Technology Cybersecurity Framework incident response functions, and that updates based on the results of incident response testing are applied to the Incident Response Plan and/or other organizational plans, to include the Cybersecurity Event Recovery Plan.

FDIC COMMENTS AND OIG EVALUATION

On August 25, 2026, the FDIC Chief Information Officer and Acting Chief Information Security Officer provided a written response to a draft of this report, which is presented in its entirety in Appendix 3.

In its response, the FDIC concurred with all four recommendations and communicated plans to complete all corrective actions by July 31, 2027. The OIG assessed the FDIC's proposed corrective actions and determined they were sufficient to address the intent of the recommendations. We consider these recommendations to be resolved. The recommendations in this report will remain open until we confirm the corrective actions have been completed and the actions are responsive. A summary of the FDIC's corrective actions is contained in Appendix 4.

APPENDIX 1: OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of our audit was to determine to what extent the FDIC has implemented processes to detect, respond, and actively defend against cyber threats.

We conducted this performance audit from April 2025 through July 2026 in accordance with the Government Accountability Office's (GAO) Generally Accepted Government Auditing Standards. Those 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.

Scope and Methodology

To test the FDIC's incident response capabilities, we established a Rules of Engagement[28] between the CIOO and OIG to perform adversarial emulation tests covering six tactics commonly used by threat actors: (b) (7)(E) [redacted]. We performed these tests using the open-source emulation tool *Invoke-Atomic*[29] that uses a PowerShell framework for developing and executing Atomic Red Team[30] tests. The FDIC provided our OIG auditors with production environment laptops [31] with the emulation tool installed locally. On our test machines, we had local administrator access[32] and configured the machine to simulate an assumed breach style testing environment. We performed our emulated testing of the FDIC's detection capabilities during September 2025.

As part of the agreed-upon Rules of Engagement, we agreed that testing endpoints should not be isolated where simulated tactics and techniques have been detected by the SOC to allow for continued OIG testing. Detected simulated activities would not be reported outside the organization (i.e., to U.S. Computer Emergency Readiness Team). If detected, the SOC would

[28] Defined as detailed guidelines and constraints regarding the execution of information security testing. The Rules of Engagement is established before the start of a security test and gives the test team authority to conduct defined activities without the need for additional permissions.
[29] Invoke-Atomic is a PowerShell module for developing and executing Atomic Red Team tests.
[30] Atomic Red Team is an open-source library of small, portable, and simple detection tests mapped to the MITRE ATT&CK® framework.
[31] A production laptop is an enterprise-managed, fully configured computing device assigned to a user for performing official work tasks in a production (i.e., real business) environment.
[32] The Administrator account has full control of the files, directories, services, and other resources on the local device. The Administrator account can create other local users, assign user rights, and assign permissions. The Administrator account can take control of local resources at any time by changing the user rights and permissions.

acknowledge this activity as a simulation test and the SRT would document the containment, eradication, and recovery steps that would be performed as if this were a real event in the security response ticket.

As part of our emulation test procedures, we had read-only access to the FDIC's SIEM to assess the FDIC's detection and response capabilities by monitoring the SIEM for notable events from our target machines, inspecting the event ticket details, and assessing security response tickets, if applicable. We determined that an emulated test went undetected if the SIEM did not generate a notable event based on EDR (i.e., (b) (7)(E)) logs. Our testing activity was captured using the Invoke-Atomic logs and these results were provided to FDIC management for risk mitigation.

We assessed the implementation of the FDIC's Insider Threat and Counterintelligence program. As part of this area, we also assessed the FDIC's logical access controls and timely removal of involuntarily separated employees. We did this by obtaining a list of individuals terminated during calendar year 2025. We then compared this listing to all logical access removals for the same period to identify the time between termination and access removal.

As part of our procedures around involuntary separations, we observed that the tracking report generated through the FDIC's (b) (7)(E) and maintained by the Division of Administration for involuntary separations did not include a time of notification of separation to the employee. Consequently, this limited us from determining the amount of time elapsed between the notice of separation and removal of logical access.

In assessing the FDIC's updates to its incident response plans, we obtained the IRP and other organizational plans including the BRP and CSER, as of 2025. We also obtained documentation of tabletop and purple team exercises as of the same period. We inspected the respective plans for updates based on the results of any tests conducted by the FDIC and assessed against the requirements in NIST 800-53, Revision 5 and against the NIST Incident Response Lifecycle under NIST 800-61, Revision 3.

Further, to accomplish our objective, we also performed the following procedures:

- Reviewed documentary evidence to assess EDR coverage as of March 2025.
- Drafted walkthrough documents of data loss prevention processes.
- Inspected documentation supporting incident handling procedures.
- Identified post-incident analysis procedures, including lessons learned.
- Assessed the FDIC's use of threat intelligence.
- Reviewed implementation of automated response capabilities as of March 2025.
- Reviewed threat hunting procedures between August 2024 - August 2025.
- Assessed risks within the vulnerability management program as of December 2025.
- Conducted interviews of responsible FDIC officials.

- Reviewed contract awards for the FDIC's Managed Security Services Provider and Security and Privacy Professional Services contractor as of 2025.

Further, we reviewed relevant Federal laws, regulations, and guidance, as well as best practices, related to incident detection and response, including:

- Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073, Dec. 18, 2014, codified at 44 U.S.C. § 3551 *et. Seq.*
- Computer Fraud and Abuse Act, Pub. L. No. 98–473, § 2102(a), 98 Stat. 2190, Oct. 12, 1984, codified at 18 U.S.C. § 1030
- Executive Order 14028, *Improving the Nation's Cybersecurity* (May 2021)
- Office of Management and Budget (OMB) M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities*
- OMB M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* (October 2021)
- OMB Circular No. A-123 *Management's Responsibility for Internal Control*
- OMB Circular No. A-130 *Managing Information as a Strategic Resource*
- *NIST Cybersecurity Framework Version* 2.0
- NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide*, August 2012
- NIST SP 800-61 Revision 3, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management*, April 2025
- NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*
- *Federal Incident Notification Guidelines* (April 2017)
- *CISA's Best Practices for MITRE ATT&CK® Mapping* (January 2023)
- *CISA's Managing Risk of Adverse/Involuntary Employee Separations*, 2024 Edition
- CISA's BOD 19-02: *Vulnerability Remediation Requirements for Internet-Accessible Systems* (April 2019)
- CISA BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities (November 2021)
- MITRE ATT&CK® Enterprise Framework v18

In addition, we reviewed relevant FDIC policies, procedures, and guidance, and compared them to identified criteria and best practices:

- FDIC Directive 1360.12, *Reporting Information Security Incidents* (August 29, 2023)
- FDIC Directive 1360.15, *Access Control for Information Technology Resources* (November 10, 2024)
- FDIC Directive 1600.7, *FDIC Insider Threat and Counterintelligence Program* (June 30, 2021)

- FDIC Directive 2150.01, *Pre-Exit Clearance for Employees* (January 13, 2025)
- *FDIC's Incident Response Plan* (February 29, 2024)
- FDIC's Breach Response Plan (June 2025)
- *FDIC's Cyber Security Event Recovery Plan* (June 22, 2018)
- *FDIC Security Response Team Playbooks*

The scope of this audit did not include an assessment of the FDIC's Managed Security Services Provider, the Security and Privacy Professional Services contractor, or other related contract activities. Any findings or recommendations contained herein should not be interpreted as an assessment of contracted services.

Work Related to Internal Controls

We determined that internal controls were significant to the audit objective. [33] In conducting this audit, we obtained an understanding of internal controls necessary to meet our audit objective. We assessed the components of internal control and identified the key components and underlying principles that were significant to achieving the audit objective as described in **Table 3**.

Table 3: Internal Control Components and Principles Identified as Significant

Components	Principles
Control Environment	Establish Structure, Responsibility, and Authority
Risk Assessment	Identify, Analyze, and Respond to Risk Assess Fraud Risk Analyze and Respond to Change
Control Activities	Design Control Activities Design Activities for the Information System Implement Control Activities
Information and Communication	Communicate Internally Communicate Externally
Monitoring	Perform Monitoring Activities Remediate Deficiencies

Source: OIG analysis of internal control components and principles using OMB Circular No. A-123 Management's Responsibility for Internal Control

Internal control deficiencies identified during the audit that were significant within the context of

[33] Internal control standards were recently emphasized by the OMB in Revised Circular No. A-123, Management Responsibility for Internal Control (March 10, 2026).

the audit objectives are presented in this report.

In addition, we determined that information system controls were significant to the audit objective. In conducting this audit, we obtained an understanding of information system controls necessary to meet our audit objective. We assessed the security and privacy controls that were significant to achieving the audit objective as described in **Table 4**.

Table 4: Information System Controls Identified as Significant

Control Group	Control Description
Access Control **[Finding 2]**	**AC-1 Policy and Procedures** requires agencies to develop, document, and disseminate access control policies and procedures that address the controls in the AC family that are implemented within systems and organizations. **Finding 2**
Configuration Management	**CM-8 System Component Inventory** requires agencies to develop and document an inventory of system components.
Incident Response **[Finding 1 and Finding 3]**	**IR-3 Incident Response Testing** requires agencies to test the effectiveness of the incident response capability. **IR-4 Incident Handling** requires agencies to implement an incident handling capability for incidents that is consistent with the incident response plan. **IR-5 Incident Monitoring** requires agencies to document incidents, including maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics as well as evaluating incident details, trends, and handling. **Finding 1** **IR-8 Incident Response Plan** requires agencies to develop an incident response plan and update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing. **Finding 3**
Program Management	**PM-12 Insider Threat Program** requires agencies to implement an insider threat program. **PM-16 Threat Awareness Program** requires agencies to implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.
Risk Assessment	**RA-5 Vulnerability Monitoring and Scanning** requires agencies to monitor and scan for vulnerabilities and remediate legitimate vulnerabilities in accordance with an organizational risk assessment. **RA 10 Threat Hunting** requires agencies to establish and maintain a cyber threat hunting capability to search for indicators of compromise.
System and Communications Protection	**SC-7 Boundary Protection** requires agencies to monitor and control external communications using techniques such as data loss and data leakage prevention tools.

Source: OIG analysis of internal controls from NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

Note: The FDIC implemented effective controls in eight security areas we identified as significant to our objective. However, in three separate control areas (IR-5 Incident Monitoring, AC-1 Policy and Procedures, IR-8 Incident Response Plan), we found the FDIC could strengthen its existing controls.

Computer Processed Data/Data Reliability

We relied on computer processed information for system-generated reports pertaining to the separated employees. To assess the reliability of this data, we corroborated information provided by management to support our audit conclusions by obtaining documentary and testimonial evidence over the reliability of the data. As a result, we determined that the information is sufficiently reliable for the purposes of our report.

Prior Office of Inspector General Reports

We reviewed the following FDIC OIG reports related to the audit findings:

- *Preventing and Detecting Cyber Threats* (Report No. AUD-19-005) The audit objective was to assess the effectiveness of the FDIC's network firewalls and SIEM tool in preventing and detecting cyber threats. Cotton and Company LLP identified weaknesses that limited the effectiveness of the FDIC's network firewalls and SIEM tool in preventing and detecting cyber threats. Our report contained 10 (closed) recommendations intended to strengthen the effectiveness of the FDIC's network firewalls and SIEM tool in preventing and detecting cyber threats.

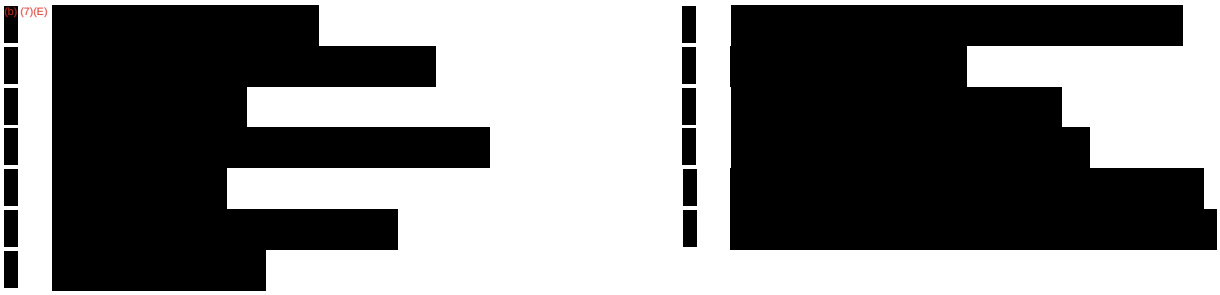
- *The FDIC's Information Security Program – 2023* (Report No: AUD-23-004) Cotton determined that the FDIC's overall information security program was operating at a Maturity Level 4 (Managed and Measurable) with respect to the FY 2023 FISMA Metrics. Our office issued a recommendation that the FDIC implement process improvements to ensure prompt notification and removal of user network accounts on or before the user's separation date.

- *The FDIC's Information Security Program – 2025* (Report No. EVAL-25-03) KPMG LLP determined that the FDIC's overall information security program was operating at a Maturity Level 4 (Managed and Measurable) with respect to the FY 2025 FISMA Metrics. KPMG found that the FDIC established several information security program controls and practices that were consistent with FISMA requirements. However, the report describes security control weaknesses that diminished the effectiveness of certain aspects of the FDIC's information security program and practices.

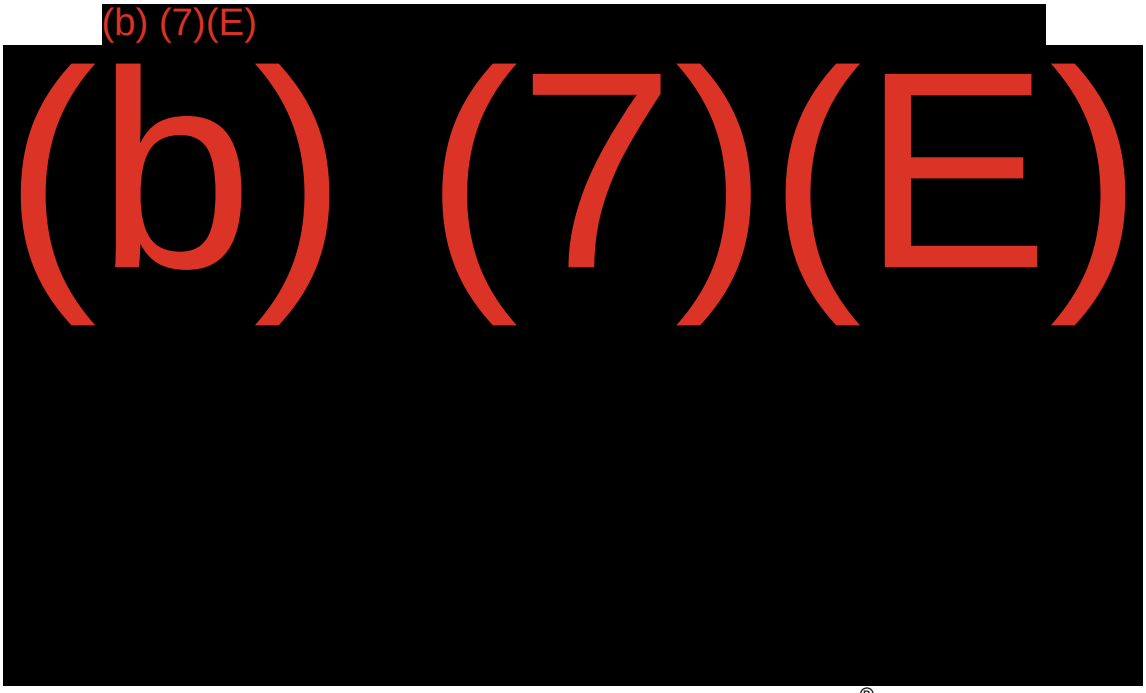
- *Review of the FDIC's Ransomware Readiness* (Report No. REV-24-01) The objective of this review was to assess the adequacy of the FDIC's process to respond to a ransomware incident. Overall, we determined that the FDIC had an adequate process to respond to a ransomware incident and generally followed applicable guidance and best practices within the five control areas that we assessed.

APPENDIX 2: EMULATED MITRE ATT&CK® TEST RESULTS

The FDIC's SIEM tool, (b) (7)(E), failed to generate notable events from ingested (b) (7)(E) logs for 45 (90 percent) of our 50 adversarial emulated tests based on the MITRE ATT&CK® Enterprise Framework Techniques. Our procedures covered 13 techniques listed below.



In some cases, other security tools such as (b) (7)(E) generated notable events. However, our scope focused on EDR logging and monitoring capabilities in (b) (7)(E) because it was the primary EDR tool that was implemented at the time of testing. **Figure 3** summarizes our emulation tests performed and MITRE ATT&CK Framework coverage and displays the tactic and techniques in which the FDIC's SIEM did not generate notable events from ingested EDR logs.



Source: OIG Analysis of Emulated Testing Results using the MITRE ATT&CK® Framework v18

APPENDIX 3: FDIC COMMENTS

FDIC Federal Deposit Insurance Corporation

MEMO

TO: Jason Yovich
Acting Assistant Inspector General
Office of Inspector General

FROM: Zachary N. Brown
Chief Information Officer, Chief Privacy Officer, and
Director, Division of Information Technology

ZACHARY BROWN Digitally signed by ZACHARY BROWN Date: 2026.08.25 17:05:14 -04'00'

Rami Dillon
Acting Chief Information Security Officer

RAMI DILLON Digitally signed by RAMI DILLON Date: 2026.08.25 16:07:03 -04'00'

CC: Nicholas Thottam, Acting Deputy CIO for Management
Jill Lennox, Chief Risk Officer
Eric Gold, Assistant General Counsel

DATE: August 25, 2026

RE: Audit of the FDIC's Incident Detection and Response Program (No. 2025-007)

Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report, entitled *Audit of the FDIC's Incident Detection and Response Program (No. 2025-007)*. The objective of the review was to determine to what extent the FDIC implemented processes to detect, respond, and actively defend against cyber threats. The FDIC appreciates the OIG's recommendations and remains fully committed to continuously enhancing its incident detection and response program to address evolving cyber threats and ensure the continued protection of the FDIC's information systems and operations.

We are pleased that the OIG's evaluation found that the FDIC has implemented effective controls in eight security areas the OIG identified as significant to its objective, demonstrating the maturity and effectiveness of the FDIC's incident detection and response program. These results suggest that the FDIC has established a strong foundation of preventive, detective, and responsive cybersecurity capabilities that support the FDIC's mission to maintain stability and public confidence in the nation's financial system.

Since the commencement of the audit, the FDIC continued to strengthen its cybersecurity posture through several significant enhancements. The FDIC completed the agency's transition to a new enterprise endpoint detection and response (EDR) platform, in order to provide enhanced threat detection, prevention, and response capabilities. Additionally, the FDIC updated its Incident Response Plan to align with guidance contained in the National Institute of Standards and Technology (NIST) Special Publication 800-61 Revision 3. As a result, the agency's incident response program now reflects current federal cybersecurity best practices and incorporates more modern incident handling and recovery principles.

Notwithstanding these enhancements, the OIG's evaluation identified opportunities for improvement in the FDIC's current controls and processes covering its incident detection and response program, as follows: (1)

FDIC Federal Deposit Insurance Corporation

strengthen its monitoring of EDR logs to better detect known adversarial techniques such as running malicious code, maintaining access, and avoiding detection; (2) update its policies for involuntarily separated employees to address the elevated risk present when an employee is involuntarily separated; and (3) better align its incident response capabilities testing to NIST standards while improving coordination within the Chief Information Officer Organization (CIOO).

Management Response to the Recommendations

The OIG's report contains three findings and four recommendations addressed to the CIO and Assistant General Counsel. FDIC management concurs with all four recommendations. A summary of our planned corrective actions and associated milestones follows.

Recommendation 1 -

We recommend that the CIO:

Update the FDIC's content development process based on emulated tests that did not generate notable events to identify where gaps in coverage exist within incident detection strategies.

Management Decision: Concur

Corrective Action: The CIOO will update its content development standard operating procedures to require the evaluation of emulated test results to identify and address gaps in incident detection coverage. The CIOO will implement the updated process during its next bi-annual use case review and document the results.

Estimated Completion Date: March 31, 2027

Recommendation 2 -

We recommend that the CIO:

Review current access permissions on FDIC endpoints and update permissions accordingly to prevent unauthorized users from disabling or interfering with endpoint detection and response services.

Management Decision: Concur

Corrective Action: The CIOO has implemented the recommendation as part of the deployment and authorization of its new EDR solution. The CIOO reviewed and established role-based access permissions for the new EDR tool and completed certification of privilege access to ensure that only authorized personnel can modify or disable EDR controls. These controls are maintained through the FDIC's existing system authorization, change management, and privilege access review processes.

Estimated Completion Date: Completed (pending submission to FDIC OIG)

Recommendation 3 –

We recommend that the Assistant General Counsel:

FDIC Federal Deposit Insurance Corporation

Update applicable FDIC directives and procedural documents, to ensure that the Division of Information Technology is notified of involuntary separations at, or prior to, the time of notification to the employee, and coordinate with appropriate stakeholders to establish risk-driven timetables for revoking and disabling access.

Management Decision: Concur

Corrective Action: The FDIC's Legal Division will work with the appropriate stakeholders to update applicable FDIC directives and procedures to ensure involuntary separation notifications are communicated timely. The CIOO will update its internal processes to align with these updates and ensure access is revoked and disabled, commensurate with risk.

Estimated Completion Date: June 30, 2027

Recommendation 4 –

We recommend that the CIO:

Update the current incident response testing procedures to ensure that the testing covers all National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) incident response functions, and that updates based on the results of incident response testing are applied to the Incident Response Plan and/or other organizational plans, to include the Cybersecurity Event Recovery Plan.

Management Decision: Concur

Corrective Action: The CIOO will revise its Incident Response Testing Procedures to align with the NIST CSF Incident Response functions and formalize a process for evaluating exercise results. Following each incident response exercise, the CIOO will document lessons learned and update the Incident Response Plan, Cybersecurity Event Recovery Plan, or other supporting documentation as needed.

Estimated Completion Date: July 31, 2027

APPENDIX 4: SUMMARY OF THE FDIC'S CORRECTIVE ACTIONS

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

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	The CIOO will update its content development standard operating procedures to require the evaluation of emulated test results to identify and address gaps in incident detection coverage. The CIOO will implement the updated process during its next bi-annual use case review and document the results.	March 31, 2027	$0	Yes	Open
2	The CIOO has implemented the recommendation as part of the deployment and authorization of its new EDR solution. The CIOO reviewed and established role-based access permissions for the new EDR tool and completed certification of privilege access to ensure that only authorized personnel can modify or disable EDR controls. These controls are maintained through the FDIC's existing system authorization, change management, and privilege access review processes.	Completed (pending submission to FDIC OIG)	$0	Yes	Open
3	The FDIC's Legal Division will work with the appropriate stakeholders to update applicable FDIC directives and procedures to ensure involuntary separation	June 30, 2027	$0	Yes	Open

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
	notifications are communicated timely. The CIOO will update its internal processes to align with these updates and ensure access is revoked and disabled, commensurate with risk.				
4	The CIOO will revise its Incident Response Testing Procedures to align with the NIST CSF Incident Response functions and formalize a process for evaluating exercise results. Following each incident response exercise, the CIOO will document lessons learned and update the Incident Response Plan, Cybersecurity Event Recovery Plan, or other supporting documentation as needed.	July 31, 2027	$0	Yes	Open

[a] Recommendations are resolved when —

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

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

APPENDIX 5: ACRONYMS AND ABBREVIATIONS

BRP	Breach Response Plan
CIOO	Chief Information Officer Organization
CISA	Cybersecurity and Infrastructure Security Agency
CSER	Cybersecurity Event Recovery Plan
DIT	Division of Information Technology
EDR	Endpoint Detection and Response
ESOS	Enterprise Security Operations Section
FDIC	Federal Deposit Insurance Corporation
GAO	Government Accountability Office
IRP	Incident Response Plan
IT	Information Technology
LEAS	Labor, Employment and Administration Section
LERS	Labor and Employee Relations Section
NIST	National Institute of Standards and Technology
OCISO	Office of the Chief Information Security Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
SIEM	Security Information and Event Management
SOC	Security Operations Center
SP	Special Publication
SRT	Security Response Team

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.

FDIC OIG website | www.fdicoig.gov
X | @FDIC_OIG
Oversight.gov | www.oversight.gov