FDIC Office of Inspector General

Audit of Security Controls for a Cloud Platform and Application

Office of Audits

September 2025 | AUD-25-02

REDACTED VERSION
PUBLICLY AVAILABLE

The redactions in this report are based on legal provisions protecting sensitive information.

Office of Inspector General

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.

Office of Inspector General

Date: September 25, 2025

Memorandum To: Sylvia W. Burns
Chief Information Officer

(b) (6)

From: Matthew Simber
Acting Assistant Inspector for Audits

Subject **Audit of Security Controls for a Cloud Platform and Application** | Report No. AUD-25-02

Enclosed is the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) report on the *Audit of Security Controls for a Cloud Platform and Application*.

The FDIC OIG contracted with the independent certified public accounting firm, Sikich CPA LLC (Sikich), to conduct a performance audit of the security controls for a cloud platform and application. The contract required Sikich's audit work to be conducted in accordance with Generally Accepted Government Auditing Standards. Our objective was to assess the effectiveness of security controls for the (b) (7)(E) cloud platform and (b) (7)(E) application.

Sikich is responsible for the enclosed report. The OIG reviewed Sikich's report and related documentation and inquired of its representatives. Our review was not intended to enable the OIG to express, and we do not express, an opinion on the matters contained in the report. Our review found no instances where Sikich did not comply with the Generally Accepted Government Auditing Standards issued by the Comptroller General of the United States.

We appreciate the cooperation and courtesies the FDIC Chief Information Officer Organization management and personnel extended to the OIG and Sikich during this audit. If you have any questions, please contact me at (703) 562-6060.

Executive Summary

Audit of Security Controls for a Cloud Platform and Application AUD-25-02 September 25, 2025

What We Did

We engaged Sikich CPA LLC (Sikich) to conduct a performance audit of security controls for a cloud platform and application. The objective was to assess the effectiveness of security controls for the (b) (7)(E) platform and (b) (7)(E) application. To address this objective, Sikich performed tests of nine IT security control areas for the cloud platform and application. Sikich also assessed policies and procedures, conducted interviews of responsible officials, and conducted penetration testing procedures.

Impact on the FDIC

The benefits of cloud computing do not eliminate the FDIC's responsibility to effectively manage security risks. The FDIC continues to expand its cloud presence by migrating its mission essential and mission critical applications into the cloud. The FDIC must ensure that its systems and data within the cloud are secured and that control weaknesses are effectively addressed. Failure to do so could result in damage and harm to FDIC systems and data, hindering its ability to maintain stability and confidence in the nation's financial system.

Results

Sikich found that the FDIC had effective controls in seven of nine security control areas assessed. However, Sikich determined that the FDIC had not effectively implemented security controls in the cloud platform and application in two areas: Identity and Access Management and Protecting Cloud Secrets. The report includes seven technical findings for the cloud platform and application attributed to two overarching themes:

1. **Insecure Coding Practices**: The FDIC teams developing cloud platforms did not consistently implement secure coding practices or functions.
2. **Cloud Service Provider Vulnerabilities:** The Cloud Service Provider was solely responsible for causing certain vulnerabilities and should be responsible for their remediation.

Sikich also mapped the seven security weaknesses identified to the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 functions (Govern, Identify, Protect, Detect, Respond, and Recover) to understand how the weaknesses impacted the FDIC. The NIST Cybersecurity Framework was designed to help organizations of all sizes and sectors manage and reduce their cybersecurity risks.

Recommendations

Sikich made eight recommendations related to the identified control deficiencies and security weaknesses that, if effectively addressed, should strengthen the security controls for the cloud platform and application. The FDIC concurred with all eight recommendations and plans to complete all corrective actions by March 31, 2026.

We also advised that the FDIC consider the existence of the continued themes of weaknesses identified during this audit that were also identified within our previous *Audit of Security Controls for the FDIC's Cloud Computing Environment* (AUD-24-01).

Audit of Security Controls for a Cloud Platform and Application

September 2025 | AUD-25-02

Part I

****

Report by Sikich LLC

PERFORMANCE AUDIT OF SECURITY CONTROLS FOR A CLOUD PLATFORM AND APPLICATION

SUBMITTED TO THE

FEDERAL DEPOSIT INSURANCE CORPORATION

AUDIT REPORT

SEPTEMBER 25, 2025

FINAL REPORT

Table of Contents

Figures

Tables

Matthew Simber
Acting Assistant Inspector General for Audits
Office of Inspector General
Federal Deposit Insurance Corporation

Subject: Audit of Security Controls for a Cloud Platform and Application

Sikich CPA LLC (Sikich) is pleased to submit the attached report detailing the results of our performance audit of the security controls for the Federal Deposit Insurance Corporation's (FDIC) (b) (7)(E) Cloud Platform and (b) (7)(E) Application. The FDIC Office of Inspector General (OIG) engaged Sikich to conduct this performance audit. Sikich performed the work from January 2025 through September 2025.

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,

Sikich CPA LLC

Sikich CPA LLC
Alexandria, VA

Introduction

The Federal Deposit Insurance Corporation (FDIC), like other Federal agencies, has increasingly adopted cloud services to support its business functions. As of July 2025, the FDIC has migrated several of its mission essential and mission critical applications[1] into a cloud environment. There are many benefits for organizations like the FDIC to migrate to the cloud; notably, the cloud service provider (CSP) has some responsibility for security, lessening the administrative overhead for the FDIC. However, as a cloud customer, the FDIC is still accountable for ensuring that its systems and data that operate in the cloud are secured in accordance with its own security standards.

The (b) (7)(E) platform, named (b) (7)(E) (hereinafter referred to as "Platform") within the FDIC at the time, supported one (b) (7)(E) application named (b) (7)(E) (hereinafter referred to as "Application"). (b) (7)(E)

In September 2024, the FDIC OIG issued a report[3] on the *Audit of Security Controls for the FDIC's Cloud Computing Environment*. In that audit, we assessed security controls on (b) (7)(E) cloud platforms and one Application Program Interface (API) platform. For that audit, our scope originally included a (b) (7)(E) cloud platform – Platform. We decided not to perform Platform and Application testing because the Application was undergoing a (b) (7)(E) at that time, including the addition (b) (7)(E) users (b) (7)(E)

Additionally, in (b) (7)(E), the FDIC deployed the first in a series of planned releases for (b) (7)(E) application, (b) (7)(E) on the Platform. (b) (7)(E) , which is one of the FDIC's core functions and is critical to the FDIC's ability to

[1] According to the FDIC Security Categorization Worksheet (March 2021), a mission essential application is defined as an application whose loss would cause a stoppage of the core operations supporting the FDIC's mission. It also defines a mission critical application as an application whose loss would produce a significant impact on the FDIC's operations, but not its core mission.

[2] Due to the sensitive nature of the report, when referring to the (b) (7)(E) vendor itself or names of services that it natively provides throughout this report, it will be referred to as "Provider."

[3] Audit of Security Controls for the FDIC's Cloud Computing Environment

(b) (7)(E) . Therefore, any disruption to the Platform would substantially hinder the FDIC from accomplishing its mission.

The objective of this audit was to assess the effectiveness of security controls for the Platform and Application. **Appendix I** contains information about the objective, scope, and methodology for this audit.

Background

Platform and Application

The Platform is a Platform-as-a-Service that provides a (b) (7)(E) environment (b) (7)(E) . The Platform features are targeted at helping organizations (b) (7)(E) Both the Platform and Application were formally authorized to operate in (b) (7)(E).

In (b) (7)(E) , the FDIC deployed (b) (7)(E) application, (b) (7)(E) on the Platform.[4] (b) (7)(E) – when all its features are implemented, which is planned to be completed by (b) (7)(E) will replace the functionality of approximately (b) (7) different legacy systems.

Support for the Platform is carried out by an FDIC platform team ("platform team") that is responsible for the FDIC's security settings at the cloud platform level. The platform team also manages the

[4] The first phase of (b) (7)(E) went live in (b) (7)(E) after the audit was scoped and was therefore excluded from our scope.

implementation of Provider objects, such as plugins,[5] process models,[6] and web APIs (see **Figure 2** below). The platform team communicates with the Provider vendor for security and performance-related subjects.

Within the FDIC, there is a Application project team ("application team") that develops and maintains the functionality of the Application for users as part of the (b) (7)(E) process. There are two primary categories of functional users:

1. Internal Users: FDIC Employees who have access to all documents within the Application, regardless of the (b) (7)(E) that they are associated with.
2. External Users: Users from (b) (7)(E) who have Application access to streamline communications during (b) (7)(E) . External user access is limited to the documents that are relevant to the user's corresponding (b) (7)(E) .

Web Application Architecture

Cloud platforms constitute an alternate method to deliver system functions, most notably web applications. Web applications generally consist of three components:

1. Web Servers – display application content on a user's browser.
2. Application Servers – logically translate user requests into a system response.
3. Databases – hold the underlying data supporting the application.

As illustrated in **Figure 1** below, when a user accesses a web application (e.g., fdic.gov), their browser sends an API[7] request to the application's web server. It will then display content generated by the web server. This content may include both static content (e.g., text in the title "About the FDIC") and interactive dynamic content that responds to user actions (e.g., the search bar at the top of the site).

---

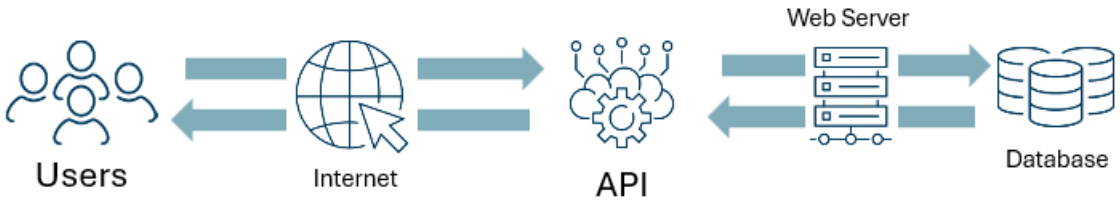
[5] Plugins provide additional functionality on top of what the Provider base platform provides. For example, one plugin on the Platform allows Provider customers to upload files (b) (7)(E) . Provider customers can download plugins from the Provider (b) (7)(E) plugins are developed either by Provider themselves or by third parties; regardless, the presence of a plugin (b) (7)(E) indicates that it passed Provider's plugin review process.

[6] Within the Provider platform, a process model is a visual representation of a sequence of automated steps. (b) (7)(E) , Provider customers can develop custom automated processes that execute upon certain triggers. For example, a customer can create a process model to automatically send an email when a user completes a form.

[7] An API is a software intermediary that allows two software components to communicate with each other using a set of definitions and protocols.

When a user interacts with dynamic content (e.g., searches for content with the word “bank”), the browser will send additional API requests to the web server that forwards this request to the application server. The application server will perform actions based on this request, which often involves querying the database to obtain information. It retrieves this information and sends it back to the web server, which displays the response on the user’s browser. In the example of searching for “bank” on fdic.gov, it would return the results from a scan of the web pages within fdic.gov.

Figure 1: Web Application Diagram



There are primarily two sections of this process that require code development:

1. The “front-end” controls for how the user views the application on their browser.
2. The “back-end” controls for the application logic. Specifically, it dictates how the application uses its resources (e.g., querying the database) to fulfill user requests.

As part of its core feature set, the Platform allows developers to create (b) (7)(E) which are custom pathways to the back end.

The open-ended nature of application development can result in numerous vulnerabilities. A sufficiently knowledgeable and motivated attacker can exploit insecure code to perform actions that were not intended by the developers. Therefore, organizations must securely develop code to mitigate the risk of such attacks. Organizations must also securely configure web servers, application servers, and databases in accordance with organizational policies and best practices. Further, organizations must implement administrative controls (e.g., access management and configuration management policies) to ensure secure usage.

DevSecOps (Development, Security, and Operations) and AppSec (Application Security)

To help facilitate faster code deployment, the FDIC is in the midst of its multi-year adoption of DevSecOps (Development, Security, and Operations), a software development practice that, through automation, continuously integrates security practices throughout the entire lifecycle of software development, from design to deployment and maintenance. This integration includes the implementation of automated code scanning tools and the collaboration of developers with security teams to identify software vulnerabilities. These practices require security assessments to be incorporated throughout the continuous integration and continuous delivery (CI/CD) process. According to the FDIC Target State Architecture plan, published in January 2025, the FDIC is planning to fully implement DevSecOps by 2027.

AppSec is the process of finding, fixing, and preventing security vulnerabilities at the application level, as part of the software development processes. AppSec and DevSecOps complement each other and are

not mutually exclusive. AppSec focuses on securing applications, while DevSecOps ensures that security is integrated across the development process. A dedicated AppSec team has a crucial role in ensuring the security of applications throughout their lifecycle. This team complements the role of existing security teams within DevSecOps. They are responsible for helping to define security requirements, integrating security requirements into software, monitoring checkpoints, promoting secure coding practices, and security testing and threat modeling for applications. The AppSec team helps to ensure that software vulnerabilities and security weaknesses are being identified and managed appropriately.

Cloud Controls Assessed

We assessed the effectiveness of the FDIC's controls to protect its cloud environments in nine areas.[8] We identified these areas based on our analysis of relevant National Institute of Standards and Technology (NIST) security standards and guidance, FDIC policy and guidance, Provider best practices, and government-wide security policy requirements. Note, that while our intended scope was exclusive to the FDIC's responsibilities as a cloud customer, our penetration testing procedures also resulted in the identification of weaknesses where the Provider vendor has responsibility for remediation. **Table 4** in **Appendix I** contains additional information about the cloud security control areas we tested and the associated criteria.

We performed penetration testing procedures over the Platform and the Application. Prior to the start of testing, we obtained concordance from key Chief Information Officer Organization (CIOO) stakeholders to conduct this testing, which was codified in a Rules of Engagement. Additionally, the CIOO created virtual desktops using Virtual Desktop Infrastructure (VDI) environments; we used the privileged accounts granted to us in these environments to install a series of primarily open-source and commercially available penetration testing tools.

We also inquired of the Platform and Application personnel regarding the key technical and functional roles for their respective systems. Based on these discussions, we requested and were provided access to key roles within the testing environment for the Platform and Application to validate effective security controls from multiple user perspectives. We also used open-source software to perform technical testing on the Platform and Application that deviate from those of a typical user and

[8] See **Appendix I**. We also assessed the effectiveness of 12 internal control principles as described in **Table 3** in **Appendix I** and defined in GAO's *Standards for Internal Control in the Federal Government* (the Green Book) (September 2014) that we deemed significant to the audit objective and relevant to the nine control areas we tested.

attempted to push the boundaries of intended access assigned to user roles. See **Appendix I** for more information about our testing procedures. Our findings reflect the observations that could be achievable by a technically proficient actor with a general understanding of the Platform and Application functions and with access to multiple user accounts.

Prior Related Audit Work

In September 2024, we issued AUD-24-01: *Audit of Security Controls for the FDIC's Cloud Computing Environment*. From June 2023 to January 2024, we performed technical testing on [redacted] cloud platforms and one API platform. We identified system-specific findings with corresponding recommendations. Despite the different cloud delivery models, platform and application team personnel, and application purposes, we identified commonalities across the findings, which we grouped into six themes: (1) insecure coding practices, (2) misconfigured security settings, (3) least privilege violations, (4) outdated software versions, (5) ineffective monitoring, and (6) Cloud Service Provider (CSP) vulnerabilities.

We noted that a contributing cause for these security findings was that the FDIC did not have [redacted]. Additionally, [redacted] were contributing causes to many of the security weaknesses that were identified.

Audit Results

Although we found that the FDIC had effective controls in seven of nine security control areas assessed (see **Table 4** for the list of control areas), we determined that the FDIC had not effectively implemented security controls in the Platform and Application in two areas – identity and access management and protecting cloud secrets. Specifically, we identified seven findings across the Platform and Application that we attributed to either the FDIC's insecure development practices or to security deficiencies within the vendor product. These findings pose risks to the confidentiality, integrity, and availability of FDIC data as a malicious user could leverage these weaknesses to exploit the Platform and Application to cause harm to the FDIC.

We provide eight recommendations related to the identified control deficiencies and security weaknesses that, if effectively addressed by management, should strengthen the security controls for

the Platform and Application. In addition, the FDIC should consider the existence of the findings and recommendations identified in this audit report with the prior findings and recommendations identified within the September 2024 audit report (AUD-24-01) when determining planned corrective actions to mitigate the weaknesses identified.

We determined that the FDIC had not effectively implemented security controls in its Platform / Application cloud computing environment for two of the nine security control areas we assessed[9] (i.e., identity and access management and protecting cloud secrets). Conversely, we found that the FDIC had effective controls in the remaining seven control areas we assessed: change management, patch management, flaw remediation, cloud-based system inventory management, cloud authorization, audit logging, and minimizing shadow-IT.[10]

As noted above, we identified a total of seven findings for the Platform and Application. Across the seven findings, we identified two common themes – those where the FDIC was responsible and those where the Provider vendor is responsible. We also mapped them to the nine security control areas that were tested:

1. **Insecure Coding Practices**: The FDIC teams developing cloud platforms did not consistently implement secure coding practices or functions. (b) (7)(E)
2. **Cloud Service Provider Vulnerabilities:** The CSP was solely responsible for causing certain vulnerabilities (b) (7)(E) and should be responsible for their remediation.

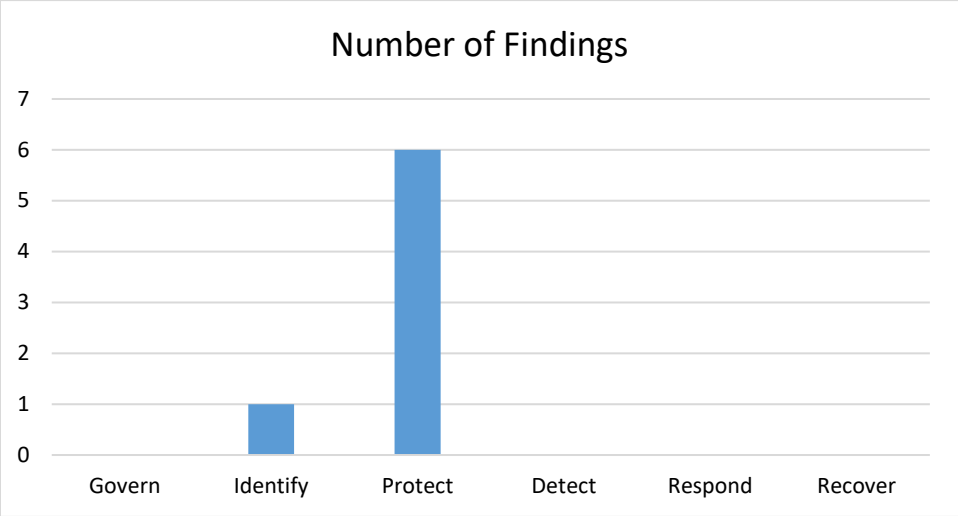
For each security weakness, we attempted to develop a proof-of-concept demonstration that a malicious user could leverage these weaknesses to cause harm to the FDIC. These proof-of-concept exploits ranged in impact level from low to high. The highest impact exploit could allow a malicious actor to (b) (7)(E), which we demonstrated could be used to, at a minimum, (b) (7)(E)

[9] See Table 4 of Appendix I for a detailed description of the nine security control areas assessed.
[10] Shadow IT is any software, hardware, or information technology (IT) resource used on an enterprise network without the IT department's approval, knowledge, or oversight.

(b) (7)(E) of our choosing. Another (b) (7)(E) exploit allowed us, as a low-level external user, to view and download any document stored within the Platform. These identified weaknesses could only be exploited by leveraging an account with legitimate access to the Platform or Application. We noted that CIOO personnel informed us that they did not identify any prior instances where any of the weaknesses identified within the themes above were exploited to compromise FDIC systems and data.

We also mapped the seven cloud security findings identified to the NIST Cybersecurity Framework (CSF) 2.0 functions (Govern, Identify, Protect, Detect, Respond, and Recover) to understand how the findings impacted the FDIC. The NIST CSF was designed to help organizations of all sizes and sectors manage and reduce their cybersecurity risks. The NIST CSF is used to provide a consistent approach for evaluating cybersecurity risks. All seven findings were aligned to the Identify and Protect functions where weaknesses related to identity and access management and protecting cloud secrets. Please refer to **Figure 3** below for further details:

Figure 3: Cloud Security Findings Compared to NIST Cybersecurity Framework Functions



Note: The scope of this audit did not include testing related to the Govern and Recover functions.

Theme #1: FDIC Insecure Coding Practices

We found that the FDIC development teams for the Platform and Application did not consistently follow secure coding practices. We identified (b) (7)(E) findings related to insecure coding practices. Specifically, we noted (b) (7)(E) where the application/platform were susceptible to (b) (7)(E) vulnerabilities (b) (7)(E) There was one

(b) (7)(E) where a (b) (7)(E) that was requested by the (b) (7)(E) application team exceeded the intended purpose of the function. See **Table 1** below for details.

(b) (7)(E)

As discussed above, the open-ended nature of web application development and the variety of application functions can leave applications susceptible to a variety of vulnerabilities. Generally, the more complex an application, the more potential for unintended behavior that can be exploited by an attacker. Mitigating the risk requires the adoption of secure coding standards. According to NIST Special Publication (SP) 800-218, *Secure Software Development Framework*, organizations should produce well-secured software with minimal security vulnerabilities in their releases. Additionally, NIST SP 800-53, Revision 5, CM-7, *Least Functionality*, states that systems should be configured to provide only essential capabilities.

We assessed the Platform and Application for susceptibility to the most common attacks, many of which are documented within the Top 10 Web Application Security Risks by the Open Worldwide Application Security Project (OWASP),[11] which is a globally recognized standard for secure web development representing the most critical security risks for web applications. We identified vulnerabilities related to the following common attacks resulting from insecure coding practices:

(b) (7)(E)

[11] See https://owasp.org/www-project-top-ten/.

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Finding #1– Unauthorized users can access documents in the FDIC's implementation of (b) (7)(E)

The Platform and Application maintain many documents as part of (b) (7)(E) These documents are stored in (b) (7)(E) The platform and application teams are responsible for ensuring that access to these documents is restricted only to those who need access to them (i.e., least privilege). NIST SP 800-53, Revision 5, AC-6, *Least Privilege*, requires organizations to provision access in accordance with this principle.

Within the context of a web application, system roles define the interactions that a user is allowed to make with the application resources. Users are expected to interact with the application via a browser user interface. Depending on the roles that users have, they will see different options within their browser.

We determined that the Platform and Application administrators appropriately developed roles in accordance with least privilege but with the assumption that users would only interact with the application via the intended method (i.e., the browser). For example, accounts belonging to external users are nominally restricted from accessing most documents in the Platform and Application. However, (b) (7)(E) they could view and download any document, including those that they are not supposed to access. Additionally, due to insecure coding practices, the platform team did not program the (b) (7)(E) below for more information.

We demonstrated this scenario when, as a low-privilege user (b) (7)(E) we downloaded (b) (7)(E) documents for a (b) (7)(E). We also downloaded documents uploaded by the Platform (b) (7)(E), including a spreadsheet (b) (7)(E). A

(b) (7)(E)

cursory test determined that (b) (7)(E) We learned that this spreadsheet was used to (b) (7)(E) Nevertheless, this highlights the overall risk posed by the lack of document-level access restrictions. In considering the impact of this finding, the FDIC should be cognizant of the risk posed by the potential exposure of (b) (7)(E) document (b) (7)(E).

Recommendation 1: We recommend the **Director, Division of Information Technology,** (b) (7)(E)

Recommendation 2: We recommend the **Director, Division of Information Technology,** limit user access by following the least privilege access principle where appropriate to documents on the cloud service provider (b) (7)(E).

(b) (7)(E)

Finding #2 – Insecure code within the Application is susceptible to (b) (7)(E) attacks

The Application contains many documents related to (b) (7)(E). To help FDIC personnel locate specific institutions and documents, the Application interface includes a search function. This search function (b) (7)(E) developed by the Application team, named (b) (7)(E) As a proof of concept, we used the (b) (7)(E), which should not be expected in regular use of (b) (7)(E).

As intended, only accounts belonging to internal users are permitted to submit inputs to the search interface. Those users are inherently permitted to view the data and files that they could obtain via this (b) (7)(E) mechanism. However, by combining this behavior with another vulnerability, it would be possible for (b) (7)(E) to leverage the vulnerability. See "Specific Exploits" below.

> **Recommendation 3:** We recommend the **Director, Division of Information Technology**, in coordination with the **Director, Division of Depositor and Consumer Protection**, (b) (7)(E)

(b) (7)(E)

Finding #3 – (b) (7)(E) plugin can be exploited (b) (7)(E)

The (b) (7)(E) plugin was developed by an FDIC contractor on the Platform team. It allows Provider customers to upload files directly to (b) (7)(E) instead of the (b) (7)(E) (b) (7)(E) which is more limited by storage. The plugin takes input such as (b) (7)(E) for a user to upload a document. (b) (7)(E) . While this capability constitutes (b) (7)(E) vulnerability, we were unable to exploit this vulnerability to obtain unauthorized access or access to information. Nevertheless, this vulnerability can still be used to communicate with (b) (7)(E) plugin is also part of a more complex exploit. See (b) (7)(E) below.

The Platform team updated the plugin (b) (7)(E) . We confirmed in June 2025 that the updated plugin addressed the risk identified in this finding. Therefore, we are not issuing a recommendation related to this finding.

Finding #4 – Users can launch (b) (7)(E)

We found that the (b) (7)(E) application team requested that a custom (b) (7)(E) called (b) (7)(E) by the Platform team. According to the Platform team, its original purpose was to facilitate on-demand document generation for (b) (7)(E). However, it is no longer used and was never identified for removal. As implemented, it can be called by (b) (7)(E) within the (b) (7)(E) and used to launch (b) (7)(E), including those that run (b) (7)(E). Additionally, (b) (7)(E) allows a user to (b) (7)(E) providing a wide range of possible attack vectors. We developed two proofs of concept demonstrating how we could exploit this (b) (7)(E) First, we used a (b) (7)(E) to send (b) (7)(E) We had full control over the contents and destination of (b) (7)(E). See **Figure 7** for an example of a (b) (7)(E):

Additionally, we targeted another (b) (7)(E). We used this ability to modify the value (b) (7)(E). Based on the set of existing (b) (7)(E). A malicious actor who could (b) (7)(E). However, given that there are (b) (7)(E), there exists even more methods by which a malicious actor can exploit the (b) (7)(E).

The Platform team removed the (b) (7)(E) after we notified them of this finding. In June 2025, we confirmed its removal through a retest. Therefore, we are not issuing a recommendation

related to this issue. However, we are including a recommendation related to the overall (b) (7)(E) apparatus.

> **Recommendation 4**: We recommend the **Director, Division of Information Technology,** identify and review the continued need for other (b) (7)(E) that provide similar capabilities to launch (b) (7)(E)

For Theme #1, these weaknesses resulted from inconsistent enforcement of secure coding practices during the development process. We noted that the (b) (7)(E) . Therefore, it is important to enforce secure coding practices with the application and platform teams.

A malicious actor who gains access to an (b) (7)(E) could exploit the insecure coding practices identified to (b) (7)(E) A malicious actor would only need to (b) (7)(E) to compromise the application.

(b) (7)(E)

During the prior *Audit of Security Controls for the FDIC's Cloud Computing Environment* report (September 2024), we identified insecure coding practices (b) (7)(E) cloud platforms similar to those listed above. We previously issued one recommendation – *Establish an enterprise* (b) (7)(E)

As discussed above, (b) (7)(E) vulnerabilities and security weaknesses (b) (7)(E).

As of July 2025, it is our understanding that the FDIC has developed a business case and funding proposal to establish (b) (7)(E) by December 30, 2025 as part of this recommendation. When this (b) (7)(E) is fully established, it will perform (b) (7)(E) on FDIC systems, including (b) (7)(E) on an ongoing basis like those identified as part of this audit.

Theme #2: Cloud Service Provider Vulnerabilities

We identified (b) (7)(E) findings that affected the security of the Platform and Application where Provider has responsibility for remediation because they have ownership and access to the underlying code. See **Table 2** below.

(b) (7)(E)

Finding #5 – (b) (7)(E)

(b) (7)(E)

We noted (b) (7)(E) officially documented functions. (b) (7)(E) it is likely that these functions present a greater attack surface within the Provider platform.

> **Recommendation 5**: We recommend the **Director, Division of Information Technology** coordinate with the vendor to mitigate the impact of (b) (7)(E)

(b) (7)(E)

Finding #6 – Provider platform is susceptible to (b) (7)(E) attacks

(b) (7)(E), we identified (b) (7)(E) we were able to (b) (7)(E) a malicious actor could (b) (7)(E)

Recommendation 6: We recommend the **Director, Division of Information Technology,** coordinate with the vendor to fix the (b) (7)(E)

(b) (7)(E)

Finding #7 – Provider (b) (7)(E)

We identified two ways to bypass the (b) (7)(E) into Provider:

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

Recommendation 7: We recommend the **Director, Division of Information Technology,** coordinate with the vendor to re-examine the need to (b) (7)(E).

Recommendation 8: We recommend the **Director, Division of Information Technology,** coordinate with the vendor to (b) (7)(E)

The findings listed above are the responsibility of the Provider to remediate, and the FDIC does not have access to the underlying source code or associated vendor processes. Therefore, we were not able to determine the cause of these findings. However, the FDIC engaged directly with the Provider vendor, who assumed responsibility for the findings listed above and took steps to address the findings.

(b) (7)(E)

The impact of these findings could result in harm to FDIC data. Specifically, the ability to exploit [redacted]

Specific Exploits Involving Multiple Vulnerabilities

Although each individual vulnerability listed above presents risks to the FDIC, many of our exploits relied on chaining together multiple vulnerabilities to create additional attack vectors. We provide examples below, alongside the associated vulnerabilities in parentheses, demonstrating specific exploitative actions that we, and by extension a malicious actor, could take to harm the FDIC:

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

- (b) (7)(E)

Other Matters

In addition to the findings above, we identified two observations (not related to the Platform or Application) when setting up our VDI[21] to perform our penetration testing procedures. We have communicated these observations to the Office of the Chief Information Security Officer (OCISO) officials, who would be responsible for taking corrective action(s).

1. (b) (7)(E)

[21] A technology that delivers a complete desktop experience (including operating system and applications) to users through a virtualized environment.

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

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

Appendix I – Objective, Scope, and Methodology

The objective of this performance audit was to assess the effectiveness of security controls for the cloud Platform and Application. Sikich conducted the audit in accordance with *Generally Accepted Government Auditing Standards* (GAGAS) (2018 revision). 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).[22] **Table 3** summarizes the principles we assessed.

Table 3: Internal Control Principles Assessed

Control Environment
Principle 3 – Establish Structure, Responsibility, and Authority
Principle 5 – Enforce Accountability
Risk Assessment
Principle 8 – Assess Fraud Risk
Principle 9 – Identify, Analyze, and Respond to Change
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 13 – Use Quality Information
Principle 14 – Communicate Internally
Principle 15 – Communicate Externally
Monitoring
Principle 16 – Perform Monitoring
Principle 17 – Evaluate Issues and Remediate Deficiencies

Source: Sikich 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

[22] 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.

have existed at the time of the audit.

We assessed the effectiveness of nine security control areas for the FDIC's cloud computing environment covered by NIST SPs and industry best practices. See **Table 4** for the control areas.

Table 4: Description of Assessed Security Control Areas

Selected Control Areas	Definition
1. **Identity and Access Management**: The FDIC has appropriately defined and assigned roles for cloud platforms and applications. Additionally, the FDIC has defined user account identities necessary to access cloud platforms and applications.	NIST SP 800-53 Rev. 5 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. NIST SP 800-53 Rev. 4 Control AC-6, *Least Privilege*, requires agencies to employ the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks. NIST 800-63-3 *Digital Identity Guidelines*, states that digital authentication is the process of determining the validity of one or more authenticators used to claim a digital identity. Additionally, it states that the use of digital identity presents a technical challenge because this process often involves proofing individuals over an open network and typically involves the authentication of individual subjects over an open network to access digital government services. There are multiple opportunities for impersonation and other attacks that fraudulently claim another subject's digital identity.
2. **Cloud Inventory Management**: The FDIC maintains an accurate inventory of assets comprising its cloud system.	NIST SP 800-53 Rev. 5 Control CM-8, *System Component Inventory*, requires agencies to develop and document an inventory of system components that accurately reflects the system, includes all components within the system, does not include duplicate accounting of components or components assigned to any other system, and is at the level of granularity deemed necessary for tracking and reporting.
3. **Cloud Authorization**: The FDIC appropriately authorized its cloud implementation based on the cloud CSP's product.	NIST SP 800-53 Rev. 5 Control CA-3, *Information Exchange,* requires agencies to approve and manage the exchange of information between the system and other systems. Additionally, NIST SP 800-53 Rev. 5 Control CA-3, *Authorization,* requires the organization to authorize the system to operate prior to commencing operations.
4. **Protecting Cloud Secrets**: The FDIC is able to configure its cloud platforms and applications to protect cloud secrets. This includes encrypting its sensitive data on cloud platforms in transit and at rest.	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. NIST SP 800-218, *Secure Software Development Framework (SSDF)*, states that organizations should produce well-secured software with minimal security vulnerabilities in its releases. Additionally, the OWASP defines common vulnerabilities endemic to web development, including injection attacks, XXS, and CSRF. NIST SP 800-53 Rev. 5 Control SC-28, *Protection of Information at Rest*, requires agencies to protect the confidentiality and integrity of information at

	rest. Additionally, Control SC-8, *Transmission Confidentiality and Integrity,* requires organizations to protect the confidentiality and integrity of transmitted information.
5. **Change Management**: The FDIC ensures that changes in cloud environments are approved prior to implementation.	NIST SP 800-53 Rev. 5 Control CM-3, *Configuration Change Control*, states that organizations need to define the types of changes to the system that should be subject to configuration control and document, test, and approve those changes with explicit consideration for security and privacy impact.
6. **Patch Management**: The FDIC is patching its cloud platforms in a timely manner.	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.
7. **Flaw Remediation**: The FDIC, as applicable, performs vulnerability scans on its cloud platforms and applications and remediates them in a timely manner.	NIST SP 800-53 Rev. 5 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.
8. **Audit Logging**: The FDIC has identified suspicious events relevant to its cloud platforms and applications. Additionally, the FDIC appropriately reviews and follows up on audit log reports.	NIST SP 800-53, Rev. 5 Controls AU-2, *Event Logging*; AU-3, *Content of Audit Records*; and AU-6, *Audit Record Review, Analysis, and Reporting;* cumulatively state that organizations should define activity they deem to be of interest; develop capabilities that log such activity; and review, analyze, and respond to incidences of the activity.
9. **Shadow-IT**: The FDIC prevents the use of unsanctioned cloud services and is able to track its usage of cloud services.	NIST 800-124 Rev. 2 *Guidelines for Management the Security of Mobile Devices in the Enterprise*, denotes Shadow-IT as staff members' work-related use of IT-related hardware, software, or cloud services without the approval, oversight, or even knowledge of the organization's IT.

Source: Sikich scoping of the audit.

We selected these nine areas because a control failure in these areas could impair the confidentiality, integrity, and availability of sensitive data on the Platform and Application. Such a failure could also impair (b) (7)(E) ability to support its business operations and communications.

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

- Assessing the extent to which FDIC policies, procedures, and guidance related to these controls aligned with NIST and government-wide security policy and guidance.
- Performing inquiries of CIOO personnel responsible for maintaining the Platform.
- Performing inquiries of CIOO personnel and (b) (7)(E) functional personnel responsible for maintaining the Application.

- Performing penetration testing procedures to identify common vulnerabilities on the Platform and Application. The procedures primarily consisted of manual analysis supported by open-source software and commercially available software such as Burp Suite Pro. We performed the following procedures:
    - Attempted access to unintended system resources using multiple types of user roles within non-production environments.
    - Obtained access to code repositories for the application to obtain a better understanding of application behavior.
    - Performed fuzz testing to determine application response to unexpected input.
    - Attempted API calls directly to the web application.
- Assessing configuration settings on each cloud platform.
- Reviewing relevant controls and responsibilities within the Provider FedRAMP package.
- Reviewing FDIC authorization packages for the Platform and Application.
- Reviewing policies and procedures, including Role-Based Access Control documents, access control policies, configuration management plans, and system descriptions.
- Obtaining relevant system output for the Platform and Application, such as audit logs, patch notes, and change tickets.

We obtained concordance from key CIOO stakeholders to conduct this testing, which was codified in a Rules of Engagement prior to performing penetration testing procedures over the Platform and Application. Additionally, the CIOO created virtual desktops using VDI environments; we used the privileged accounts granted to us in these environments to install a series of open-source and commercially available penetration testing tools. We also inquired of application personnel regarding key technical and functional roles for the Application. Based on these discussions, we requested and were provided access to key roles within the QA environment for each application to validate effective security controls from multiple user perspectives.

We used NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Federal Information Systems and Organizations* (September 2020), as the primary criteria for determining whether the FDIC had

established and implemented effective controls to secure and manage its cloud computing services. We also used NIST SP 800-53, Rev. 4 (April 2013) where applicable because the FedRAMP control baselines are still based on the older SP while transitioning to Rev. 5. We supplemented NIST SP 800-53 with other SPs including, NIST SP 800-63-3, *Digital Identity Guidelines* (June 2017); 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 800-123, *Guide to General Server Security* (July 2008); and NIST SP 800-218, *Secure Software Development Framework* (SSDF) (February 2022). We also reviewed best practices from Federal Information Processing Standards Publication 140-3, *Cryptographic Module Validation Program* (March 2019).

To support our knowledge of publicly available findings, we used the Common Vulnerabilities and Exposures (CVE) system, maintained by the U.S. National Cybersecurity Federally Funded Research and Development Center (FFRDC). Additionally, we reviewed guidelines from non-profit organizations such as the Center for Internet Security (CIS), which develops security benchmarks for software platforms, and the OWASP, which publishes articles describing common web application vulnerabilities. We also reviewed best practices published online by the Provider.

We discussed our preliminary findings and conclusions with representatives of FDIC management throughout the audit.

Audit of Security Controls for a Cloud Platform and Application

Part II

****

FDIC Comments and OIG Evaluation

September 2025 | AUD-25-02

FDIC COMMENTS AND OIG EVALUATION

On September 17, 2025, the FDIC Chief Information Officer (CIO) and Chief Information Security Officer (CISO) provided a written response to a draft of this report, which is presented in its entirety in **Appendix 1**.

In its response the FDIC concurred with all of the recommendations. The FDIC plans to complete all corrective actions by March 31, 2026. The corrective actions are sufficient to address the intent of the recommendations and we consider these recommendations to be resolved.

The recommendations in this report will remain open until we confirm that corrective actions have been completed and the actions are responsive. A summary of the FDIC's corrective actions is contained in **Appendix 2**.

APPENDIX 1: FDIC COMMENTS

FDIC Federal Deposit Insurance Corporation

MEMO

TO: Matthew Simber
Acting Assistant Inspector General for Audits
Office of Inspector General

FROM: Sylvia W. Burns
Chief Information Officer, Chief Privacy Officer, and Director,
Division of Information Technology

SYLVIA BURNS Digitally signed by SYLVIA BURNS Date: 2025.09.17 15:01:10 -04'00'

ZACHARY BROWN Digitally signed by ZACHARY BROWN Date: 2025.09.17 16:33:55 -04'00'

Zachary N. Brown
Chief Information Security Officer

CC: (b) (7)(E)
Mark F. Mulholland, Deputy Chief Information Officer for Management
Sheena Burrell, Deputy Chief Information Officer for Technology

DATE: September 17, 2025

RE: Draft Office of Inspector General Report, Entitled *Audit of Security Controls for a Cloud Platform and Application* (No. 2025-001)

Thank you for the opportunity to review and comment on the subject draft audit report. The Office of Inspector General (OIG) issued the draft report on September 4, 2025. The objective of the audit was to assess the effectiveness of security controls for the (b) (7)(E) platform and (b) (7)(E) application. The FDIC places a high priority on implementing effective security controls to ensure the confidentiality, integrity, and availability of Corporate data and systems operating in the cloud. The (b) (7)(E) cloud platform, also known as the (b) (7)(E) (b) (7)(E) supports a (b) (7)(E) application called the (b) (7)(E) (b) (7)(E) under the Division of (b) (7)(E)

To achieve its objective, the OIG performed tests of nine information technology (IT) security control areas for the cloud platform and application. The OIG also assessed policies and procedures, conducted interviews of responsible officials, and conducted penetration testing procedures. To this end, the Chief Information Officer Organization (CIOO) created virtual desktops using Virtual Desktop Infrastructure with a series of open-source and commercially available penetration testing tools and provisioned privileged accounts necessary to conduct testing. The OIG also requested and was granted access to key technical and functional roles within the Quality Assurance (QA) environment for application personnel to validate effective security controls.

As detailed in the draft report, the OIG found that the FDIC had effective controls in seven of nine security control areas assessed. Specifically, the FDIC had effective controls in change management, patch management, flaw remediation, cloud-based system inventory management, cloud authorization, audit logging, and minimizing shadow-IT. However, the OIG also found that the FDIC had not effectively implemented controls in the remaining two security control areas: identity and access management and protecting cloud secrets. The draft

1

FDIC Federal Deposit Insurance Corporation

report contains seven findings attributed to insecure development practices or security deficiencies within the vendor product and eight related recommendations to strengthen FDIC's security controls for (b) (7)(E) (b) (7)(E)

The CIOO concurs with all eight of the report's recommendations. At the time of the OIG's draft report issuance, the CIOO had completed actions to address three of the eight recommendations, and work is underway to address the remaining five recommendations. The CIOO is working to document completed actions for purposes of preparing closure packages for the recommendations. A summary of management's planned and completed corrective actions follows.

Recommendation 1

We recommend that the Director, Division of Information Technology:

(b) (7)(E)

Management Decision: Concur

Corrective Action: The FDIC will remove the (b) (7)(E) and implement a replacement that will include (b) (7)(E) The FDIC has developed and tested the fix to include (b) (7)(E) (b) (7)(E) which will be deployed in the production environment by Q4 2025.

Estimated Completion Date: March 31, 2026

Recommendation 2

We recommend that the Director, Division of Information Technology:

Limit user access by following the least privilege access principle where appropriate to documents on the cloud service provider (b) (7)(E)

Management Decision: Concur

Corrective Action: The application team updated its document download process to check user permissions and configured the document download to occur from the provider (b) (7)(E) instead of directly from (b) (7)(E) The FDIC has developed and tested the fix, which will be deployed in the production environment by Q4 2025.

Estimated Completion Date: March 31, 2026

Recommendation 3

We recommend that the Director, Division of Information Technology, in coordination with the Director, Division (b) (7)(E)

(b) (7)(E)

Management Decision: Concur

Corrective Action: The application team updated the (b) (7)(E) (b) (7)(E) vulnerability. The platform team confirmed that this update was

applied in production and addressed the vulnerability. In addition, the platform team will update its platform governance Standard Operating Procedures to require that (b) (7)(E) (b) (7)(E) attacks by Q4 2025.

Estimated Completion Date: March 31, 2026

Recommendation 4

We recommend that the Director, Division of Information Technology:

Identify and review the continued need for other (b) (7)(E) that provide similar capabilities to launch (b) (7)(E)

Management Decision: Concur

Corrective Action: The platform team will update its Software Development Life-Cycle processes to actively identify and periodically review its use of (b) (7)(E) by Q4 2025.

Estimated Completion Date: March 31, 2026

Recommendation 5

We recommend that the Director, Division of Information Technology:

Coordinate with the vendor to mitigate the impact of (b) (7)(E) (b) (7)(E)

Management Decision: Concur

Corrective Action: Completed. The vendor mitigated the impact of (b) (7)(E) (b) (7)(E) These controls ensure that (b) (7)(E) effectively neutralizing potential threats. The vendor product security team received confirmation from its third-party security assessors that the vulnerability found by the OIG was resolved within the product. The FDIC platform team confirmed that this hotfix was applied to the FDIC (b) (7)(E) environment.

Completion Date: July 22, 2025

Recommendation 6

We recommend that the Director, Division of Information Technology:

Coordinate with the vendor to fix the (b) (7)(E) vulnerability in the (b) (7)(E) (b) (7)(E)

Management Decision: Concur

Corrective Action: The vendor refactored the (b) (7)(E) to prohibit (b) (7)(E) The vendor product security team received confirmation from its third-party security assessors that the vulnerability found by the OIG

was resolved within the product. The FDIC platform team is coordinating with the vendor to implement this hotfix.

Estimated Completion Date: October 30, 2025

Recommendation 7

We recommend that the Director, Division of Information Technology:

Coordinate with the vendor to re-examine the need to (b) (7)(E)

Management Decision: Concur

Corrective Action: Completed. The OIG reported a vulnerability that could be exploited using legacy (b) (7)(E) (b) (7)(E) The vendor implemented a validation check during (b) (7)(E) which verifies a (b) (7)(E) The FDIC coordinated with the vendor for its need to support (b) (7)(E) Currently, the vendor does not have any plans to end (b) (7)(E) (b) (7)(E) The vendor product security team received confirmation from its third-party security assessors that the vulnerability found by the OIG was resolved within the product. The FDIC platform team confirmed that this hotfix was applied to the FDIC (b) (7)(E) environment.

Completion Date: August 28, 2025

Recommendation 8

We recommend that the Director, Division of Information Technology:

Coordinate with the vendor to (b) (7)(E) (b) (7)(E)

Management Decision: Concur

Corrective Action: Completed. The vendor updated configurations to set the (b) (7)(E) after a (b) (7)(E) The vendor product security team received confirmation from its third-party security assessors that the vulnerability found by the OIG was resolved within the product. The FDIC platform team confirmed that this hotfix was applied to the FDIC (b) (7)(E) environment.

Completion Date: July 22, 2025

APPENDIX 2: 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 FDIC plans to remove the (b) (7)(E) and implement a replacement that will include (b) (7)(E)	March 31, 2026	$0	Yes	Open
2	The FDIC updated its document download process to check user permissions and configured the document download to occur from the provider (b) (7)(E) instead of directly from (b) (7)(E) The FDIC has developed and tested the fix, which should be deployed in the production environment.	March 31, 2026	$0	Yes	Open
3	The FDIC updated the (b) (7)(E) vulnerability. In addition, the FDIC plans to update its platform governance Standard Operating Procedures to require that (b) (7)(E) attacks.	March 31, 2026	$0	Yes	Open
4	The FDIC plans to update its Software Development Life-Cycle processes to actively identify and periodically review its use of (b) (7)(E)	March 31, 2026	$0	Yes	Open
5	The vendor mitigated the impact of (b) (7)(E)	July 22, 2025	$0	Yes	Open

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
	(b) (7)(E) The vendor product security team received confirmation from its third-party security assessors that the vulnerability found by the OIG was resolved within the product. The FDIC confirmed that this hotfix was applied to the subject FDIC cloud environment.				
6	The vendor refactored the (b) (7)(E) The vendor product security team received confirmation from its third-party security assessors that the vulnerability found by the OIG was resolved within the product. The FDIC is coordinating with the vendor to implement this hotfix.	October 30, 2025	$0	Yes	Open
7	The vendor implemented a validation check during (b) (7)(E) which verifies a user's group membership to determine access authorization. The FDIC coordinated with the vendor for its need to support (b) (7)(E); however, the vendor does not have any plans to end (b) (7)(E) The vendor product security team received confirmation from its third-party security assessors that the vulnerability found by the OIG was resolved within the product. The FDIC confirmed that this hotfix was applied to the FDIC (b) (7)(E) environment.	August 28, 2025	$0	Yes	Open
8	The vendor updated configurations to set the (b) (7)(E) after a	July 22, 2025	$0	Yes	Open

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
	(b) (7)(E) he vendor product security team received confirmation from its third-party security assessors that the vulnerability found by the OIG was resolved within the product. The FDIC confirmed that this hotfix was applied to the FDIC (b) (7)(E) environment.				

[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.

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