Federal Housing Finance Agency
Office of Inspector General

FHFA's Disaster Recovery Exercise for Its General Support System Needs Improvement

Audit Report • AUD-2024-010 • September 25, 2024

EXECUTIVE SUMMARY

PURPOSE

Pursuant to the Federal Information Security Modernization Act of 2014 (FISMA) and National Institute of Standards and Technology (NIST) guidance, agencies must establish, maintain, and implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems. Agencies must also periodically test and evaluate their information security policies, procedures, and practices.

We performed this audit to determine whether the Federal Housing Finance Agency (FHFA or Agency) conducted its annual Disaster Recovery Exercise (DRE) in accordance with its contingency planning policy and procedures for recovering its General Support System (GSS).

RESULTS

We determined that FHFA did not effectively plan its Fiscal Year (FY) 2024 DRE for the GSS. Specifically, FHFA's contingency planning documents for the GSS were missing certain required elements and included outdated information. Additionally, FHFA did not successfully test its remote access infrastructure in November 2023 as planned, although it did conduct a successful exercise for its GSS database servers in March 2024. FHFA also did not encrypt its backup data-at-rest residing at FHFA's alternate site as required by NIST and FHFA standards.

These weaknesses create the risk that FHFA may not be able to effectively and timely recover its network and systems in the event of a service disruption or disaster. Accordingly, we are reporting three findings related to the identified control deficiencies.

RECOMMENDATIONS

We made six recommendations to address our findings. In a written response, FHFA management agreed with our recommendations.

This report was prepared by Mitul Patel, IT Audit Director; Zachary Lewkowicz, IT Audit Manager; David Peppers, Auditor-in-Charge; Brian Prisbe, Auditor; with assistance from Abdil Salah, Assistant Inspector General for Audits. We appreciate the cooperation of FHFA staff, as well as the assistance of all those who contributed to the preparation of this report. This report has been distributed to Congress, the Office of Management and Budget, and others and will be posted on our website, www.fhfaoig.gov, and www.oversight.gov.

James Hodge
Deputy Inspector General for Audits /s/

TABLE OF CONTENTS

ABBREVIATIONS

BIA	Business Impact Analysis
DRE	Disaster Recovery Exercise
FHFA or Agency	Federal Housing Finance Agency
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAO	Government Accountability Office
GSS	General Support System
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Federal Housing Finance Agency Office of Inspector General
OTIM	Office of Technology and Information Management
POA&M	Plan of Action and Milestones
SP	Special Publication

BACKGROUND

FISMA requires agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems. In addition, FISMA requires agencies to perform periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices. Pursuant to FISMA, NIST is responsible for developing standards and guidelines, including minimum requirements for federal information systems. Those information security standards provide requirements necessary to improve the security of federal information and information systems. In addition, NIST develops and issues recommendations and guidance documents called Special Publications (SP).

NIST SP 800-34, Revision (Rev.) 1, *Contingency Planning Guide for Federal Information Systems*, defines contingency planning as interim measures to recover information technology (IT) services following an emergency or system disruption. Interim measures may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods.

FHFA's Network and Systems

FHFA's Office of Technology and Information Management (OTIM) works with all mission and support offices to promote the effective and secure use of information and systems.

FHFA's network and systems process and host data and information such as financial reports, data from the Enterprises, examinations and analyses of the regulated entities, and personally identifiable information of employees. FHFA's GSS is a wide area network that provides connectivity, information sharing and data processing capabilities, remote and network access, and security and support services.

The remote access infrastructure[1] is distributed across a primary site and an alternate site to ensure redundancy and failover[2] capabilities. In the event the primary site becomes unavailable, the system will automatically failover to the alternate site. Once the primary site is restored and back online, the system will automatically failback.[3] Both the primary site and alternate site use the same infrastructure for remote access. When updates or patches are applied at the primary

[1] The remote access infrastructure gives FHFA users the ability to remotely login to the network.

[2] Failover is the capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of a previously active system.

[3] Failback is the process of returning a system to its original location after a failover.

site, it is simultaneously replicated at the alternate site ensuring consistency across the entire platform.

FHFA's GSS database servers are part of its cloud infrastructure. The database servers contain dynamic data that changes each time the database is updated. There are several databases on these servers, including the following three that FHFA intended on testing during its DRE:

- Correspondence Tracking System that captures and tracks correspondence that FHFA receives from external sources (e.g., the public, Congress, regulated entities, etc.).
- Merit Central / FHFA Performance Management System that manages merit pay increases and performance reviews.
- Affordable Housing Program Library and Inquiry System that manages and tracks questions regarding the Affordable Housing Program and the Community Investment Cash Advances Program.

FHFA's Fiscal Year 2024 Disaster Recovery Exercise

Historically, OTIM has conducted its DRE annually to test the effectiveness of contingency plans and the organizational readiness to execute those plans. According to FHFA, these plans are designed to restore computer operations within an acceptable period in the event of an incident or disaster.

The FY 2024 DRE was conducted in two distinct parts. The first part involved the failover and failback of FHFA's remote access infrastructure that was performed in November 2023. The second part involved testing automated replication of transaction logs from a primary database server to a secondary database server in March 2024.

Part One of FHFA's Disaster Recovery Exercise (November 2023)

In part one of the exercise, OTIM identified the remote access infrastructure as a critical GSS service to failover and failback on November 5, 2023. OTIM's Information System Contingency Plan team provided us with the Disaster Recovery Procedures for FHFA Production Systems

OTIM-550[4] (hereinafter referred to as recovery procedures)[5] that they would follow to conduct the exercise. After the exercise, OTIM prepared the following documents:

- DRE Test Results 2023 (February 9, 2024) that described the tests conducted and included screenshots showing evidence of their completion.
- Disaster Recovery Test Closure Memo (February 9, 2024) that detailed the purpose of the exercise, when it was completed, and the results of the test.
- OTIM After Action Report that explained major strengths and lessons learned during the exercise (attachment to the Disaster Recovery Test Closure Memo).

Part Two of FHFA's Disaster Recovery Exercise (March 2024)

In part two of the exercise, OTIM identified three GSS databases to test on March 22, 2024. OTIM's Information System Contingency Plan team provided us with the database recovery procedures that they would follow to conduct the exercise. We noted that these procedures were not included in the latest version of the recovery procedures. After the exercise OTIM prepared the following documents:

- Disaster Recovery Test Observation document (March 22, 2024) that explained the actions taken during the exercise and the results of the test.
- Updated database procedures that described the steps taken during the exercise and the results of the database queries run during the test.
- Disaster Recovery Test Closure Memo (April 5, 2024) that detailed the purpose of the exercise, when it was completed, and the results of the test.
- OTIM After Action Report that explained major strengths and lessons learned during the exercise (included as an attachment to the Disaster Recovery Test Closure Memo).

[4] Version 5.4 dated November 1, 2023.

[5] FHFA's recovery procedures constitute the Information System Contingency Plan for the GSS and provide procedures for recovering several GSS critical IT services. The recovery procedures assign the responsibility and authority to take whatever steps necessary to identify, respond, contain, and eradicate the impact of an IT disaster to the Disaster Recovery Coordinator within OTIM, in conjunction with OTIM's leadership. The recovery procedures also describe failover and failback procedures for critical GSS services and FHFA's public website.

OBJECTIVE AND SCOPE

The objective of our audit was to determine whether FHFA effectively planned and successfully conducted DREs for its GSS that provides connectivity between the Agency's sites, headquarters, and data centers, as well as internet access, email, and directory services for all Agency divisions and offices. The audit scope covered the DREs in fiscal year 2024.

RESULTS

We observed and analyzed FHFA's FY 2024 DRE and determined that FHFA did not effectively plan its exercises for the GSS. Furthermore, FHFA did not successfully test its remote access infrastructure in November 2023 as planned, but was successful in conducting the exercise for its three databases in March 2024. Specifically, we noted the following weaknesses:

- FHFA's contingency planning documents for the GSS were missing required elements and included outdated information (noted in both parts of the DRE);
- FHFA did not perform the failback part of its remote access infrastructure in accordance with its recovery procedures during part one of its DRE; and
- FHFA did not encrypt its backup data-at-rest residing at its alternate site.

These weaknesses create the risk that an effective and timely recovery of FHFA's network and systems in the event of a service disruption or disaster may not occur. As described below, we are reporting three findings.

Finding 1: FHFA Did Not Effectively Maintain Contingency Planning Documents for Its GSS

During FHFA's FY 2024 DRE we found that FHFA's contingency planning documents for the GSS were missing required elements and included outdated information. Specifically, we noted that OTIM's Business Impact Analysis (BIA)[6] and recovery procedures for the GSS were not consistent or up to date as follows:

- The BIA was not updated on an annual basis. The last BIA was conducted in May 2022. NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and*

[6] According to NIST SP 800-34, effective contingency planning begins with an agency's development of an organization contingency planning policy and a BIA of each information system. The purpose of a BIA is to correlate the information system with the critical mission and services it provides, and based on that information, characterize the consequences of a disruption. Using the BIA, agencies determine their contingency planning requirements and priorities.

Organizations (updated December 10, 2020), requires organizations to develop and periodically update the contingency plan for each information system. FHFA's Contingency Planning Standard, Rev. 2.1 (November 30, 2022), requires FHFA to review and update contingency plans at least annually, or at any time in which a change to the operating environment or significant change to recovery procedures has occurred. OTIM officials stated that the BIA was not reviewed annually because FHFA lost a contractor in August 2023 due to a reduction in force with no backfills. OTIM officials also stated they were in the process of updating the BIA.

- The recovery procedures and BIA contained inconsistent recovery objectives related to the recovery time objective[7] and recovery point objective.[8] For example, the recovery time objective for the GSS is 8 hours in the BIA but is 4 hours in the recovery procedures. Additionally, the recovery point objective for all components listed in the BIA is 1 day but is 4 hours in the recovery procedures. NIST SP 800-53 Rev. 5 requires organizations to provide recovery objectives, restoration priorities, and metrics for the resumption of the information system operations within defined time periods consistent with its recovery time and point objectives. OTIM officials stated that the times set for both objectives were inconsistently documented within the BIA and recovery procedures because these documents have not been updated. OTIM officials also stated they were in the process of updating the recovery procedures.

- The recovery procedures did not contain instructions or procedures that describe the database actions to take during a disaster recovery for the Correspondence Tracking System, the Merit Central / FHFA Performance Management System, and the Affordable Housing Program Library and Inquiry System. Although procedures were provided to us separately before performing part two of the DRE in March 2024, OTIM officials did not include them in the recovery procedures because they were not vetted and approved at the time of last update (November 1, 2023). NIST SP 800-53 Rev. 5 requires organizations to establish a contingency planning policy and procedures. FHFA's Contingency Planning Standard requires FHFA to maintain plan(s) outlining the resumption of essential mission and business functions in accordance with NIST SP 800-34. OTIM officials stated that they are working on incorporating the contingency planning procedures for the GSS databases in the next version of the recovery procedures.

- The recovery procedures did not include steps for validating a successful failover and failback of the remote access infrastructure system. NIST SP 800-53 Rev. 5 requires

[7] Recovery time objective is the targeted duration of time within which a business process must be restored after a disruption to avoid unacceptable consequences.

[8] Recovery point objective is the maximum acceptable amount of data loss measured in time before the disruption occurred.

organizations to establish a contingency planning policy and procedures. FHFA's Contingency Planning Standard requires FHFA to maintain plan(s) outlining the resumption of essential mission and business functions in accordance with NIST SP 800-34. OTIM officials stated that it was an oversight that they did not have these steps in their recovery procedures document. They further stated that these procedures will be included as part of the next version of the recovery procedures.

We also noted discrepancies between the After Action Report and DRE Test Results 2023 documents.

- The After Action Report for the remote access infrastructure portion of the DRE indicated that a failback occurred; but the Recovery Exercise Test Results 2023 (February 9, 2024) did not include screenshots showing evidence of the failback. OTIM officials stated that they did not show evidence of a failback in the test results because there was no manual intervention to witness since the failback was automatic. However, in a meeting with OTIM officials in April 2024, we were shown that OTIM had the capability to view and capture the evidence of a failback. Furthermore, an OTIM official stated that OTIM forgot to take a screenshot during the exercise to demonstrate that a failback occurred. While we were provided additional evidence showing that a failback occurred, OTIM did not update the Recovery Exercise Test Results 2023.

- The After Action Report dates for the length of part one of the DRE were listed as November 3, 2023, through November 5, 2023, but the Recovery Exercise Test Results 2023 showed that the exercise took place from November 3, 2023, through November 13, 2023. OTIM officials stated that the official end date of the exercise should be corrected to reflect November 13, 2023. The same officials added that the original planned end date of November 5, 2023, was changed due to a scheduled building-wide power outage.

NIST SP 800-53 Rev. 5 requires organizations to incorporate lessons learned from contingency plan testing, training, or actual activities into contingency testing and training. It also requires organizations to review the contingency plan test results. FHFA's Common Control Plan (May 10, 2023) requires that after the conclusion of a failover or after a functional test of the recovery procedures, an After Action Report is completed and reviewed by OTIM management. The After Action Report should include a brief summary of the exercise, observations, and lessons learned, which may result in updates to the recovery procedures. The Common Control Plan also states that the recovery procedures test results are reviewed and the plan is updated based on lessons learned.

By not effectively planning and maintaining contingency planning documentation, FHFA faces an increased risk that the organization may not be prepared to recover in the event of a disaster. Furthermore, relying on recovery procedures that may have missing, inconsistent, outdated, or

incorrect procedures could potentially result in significant data loss, ineffective recovery efforts, operational disruptions and delays, and potential financial loss due to downtime and recovery costs.

Recommendations

We recommend that the FHFA Chief Information Officer:

1. Update the BIA annually in accordance with FHFA standards.

2. Update the disaster recovery procedures document to ensure it includes (a) up to date time periods for the recovery time objective and the recovery point objective for resumption of the GSS operations consistent with the BIA, (b) database procedures, and (c) steps to validate successful failover and failback of the remote access infrastructure system.

3. Ensure the After Action Report is consistent with the Recovery Exercise Test Results by documenting all actions taken during the failover and failback of the DRE including all correct dates for when testing was conducted.

Finding 2: FHFA Did Not Successfully Test Its Remote Access Infrastructure

OTIM did not perform the 2023 DRE failback part of its remote access infrastructure in accordance with its recovery procedures. OTIM officials scheduled a screensharing virtual conference with us on November 5, 2023, to observe the failover and failback of FHFA's remote access infrastructure from the primary to the alternate site and vice versa. We observed an OTIM official follow the steps in the recovery procedures to perform a failover, which restored the system to the alternate site without disruption and within the recovery time objective. However, the OTIM official did not perform recovery procedure steps to failback the system as planned. Because our objective was to determine if FHFA followed its recovery procedures as planned, we did not interrupt or make inquiries during the exercise that could have impacted the results.

NIST SP 800-53 Rev. 5 requires that organizations test the contingency plan for the system at an organization-defined frequency using organization-defined tests to determine the effectiveness of the plan and the readiness to execute the plan. FHFA's Contingency Planning Standard, Rev. 2.1 (November 30, 2022), requires FHFA to test the contingency plans at least annually, using table-top exercises or functional exercises to determine the effectiveness of the plans and the organizational readiness to execute the plans. FHFA's recovery procedures detail specific steps to be performed for a successful failover and failback of FHFA's remote access infrastructure. Additionally, we learned from the Recovery Exercise Test Results 2023 that OTIM scheduled the following procedures, of which we were unaware:

- Transfer of the lead domain controller role from the primary to the alternate site and vice versa that occurred on November 3, 2023, and November 13, 2023; and

- Failback of the remote access infrastructure that occurred on November 13, 2023.[9]

Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government*[10] requires management to communicate quality information externally through reporting lines so that external parties can help the entity achieve its objectives and address related risks. Management should also include information related to the entity's events and activities that impact the internal control system in these communications.

An OTIM official told us that the reason the failback was not performed during our observation was because OTIM had changed their plan to perform the failback on November 5, 2023, and did not inform the OIG audit team. An OTIM official also stated that the transfer of the lead domain controller roles was not performed during our observation due to an inadvertent omission.

Upon further communication with OTIM officials we were informed that after the failover on November 5, 2023, OTIM planned to leave the system running from the alternate site until after the scheduled building-wide power outage at the primary site on November 11, 2023. OTIM then conducted the failback to the primary site on November 13, 2023.

By not conducting a DRE according to plan, FHFA may not be able to determine the effectiveness of its disaster recovery plans and the organizational readiness to execute the plans in the event of a disaster. As such, OTIM may not be fully aware of potential risks during the exercise and may not recover the system successfully or timely during a disruption. As noted in this finding, we were unable to evaluate FHFA's ability to conduct specific actions taken during its exercise because OTIM did not communicate all scheduled exercise activities, including last-minute changes.

Recommendations

We recommend that the FHFA Chief Information Officer:

4. Perform annual testing of the contingency plan in accordance with the recovery procedures document to ensure failover and failback are conducted as planned.

[9] The failback on November 13, 2023, occurred without disruption, as supported by evidence from OTIM on May 29, 2024. However, we determined that the November 2023 exercise was not successful because it was not performed as planned on November 5, 2023, in accordance with the recovery procedures.

[10] GAO-14-704G, *Standards for Internal Control in the Federal Government* (September 2014).

5. Ensure OTIM officials communicate planned DREs and any scheduled changes with all parties involved, including auditors and other independent observers.

Finding 3: FHFA Did Not Encrypt Its Backup Data-at-Rest Residing at FHFA's Alternate Site

FHFA encrypted backup data-at-rest for its primary site but did not implement encryption for all backup data-at-rest at its alternate site. Specifically, FHFA's Common Control Plan, which provided the implementation status of NIST required controls, documented that FHFA does not encrypt backup data-at-rest as required by NIST and FHFA standards.

NIST SP 800-53 Rev. 5 requires that organizations implement cryptographic mechanisms to prevent unauthorized disclosure and modification of organization-defined backup information. Furthermore, FHFA's Contingency Planning Standard, Rev. 2.1 (November 30, 2022), requires FHFA to encrypt backup information at rest.

OTIM officials informed us that they already have an open Plan of Action & Milestones (POA&M) tracking the backup data-at-rest encryption issue. The POA&M reflects that OTIM plans to replace the alternate site backup storage server with one that has a valid encryption license by September 30, 2024. We found that OTIM evaluated this issue as a low risk; however, the POA&M did not include compensating controls that reflect OTIM's assessment of low risk.

An OTIM official stated that the backup storage server located at the alternate site is no longer supported by the vendor and does not have an encryption license. The official further stated that FHFA moved most of its backup data to encrypted cloud storage services and is relying on the physical security controls provided by the alternate site data center until the backup storage server is replaced. The same official stated that OTIM would modify the existing POA&M to include physical security controls in place. Based on our observation, we found that OTIM has effective physical security controls in place at the alternate site; however the POA&M does not list out these controls.

Without encryption of data-at-rest, FHFA's information residing at its alternate site could be at risk of unauthorized disclosure and modification. Furthermore, this could expose the system to cyber threats, including data breaches, identity theft, and other cybercrimes, which can have severe legal and financial consequences.

Recommendation

We recommend that the FHFA Chief Information Officer:

6. Encrypt all backup data-at-rest at FHFA's alternate site and update the existing POA&M to include compensating controls until the POA&M has been closed.

FHFA COMMENTS AND OIG EVALUATION.....

We provided FHFA management an opportunity to review and provide technical comments to a draft of this audit report. FHFA management did not have any technical comments. In a written response, FHFA management agreed with our recommendations and plans to do the following:

1. Update the BIA by October 31, 2024.

2. Update the disaster recovery procedures document by April 15, 2025, to ensure it includes (a) up-to-date periods for the recovery time objective and the recovery point objective for resumption of the General Support Systems operations consistent with the BIA, (b) database procedures, and (c) steps to validate successful failover and failback of the remote access infrastructure system.

3. Ensure the After Action Report accurately captures the Disaster Recovery Exercise Test Results by documenting all actions taken during the failover and failback activities by April 15, 2025.

4. Perform annual testing of the contingency plan in accordance with FHFA's disaster recovery procedures and ensure failover and failback activities are conducted as planned by April 15, 2025.

5. Communicate the next planned Disaster Recovery Exercises to all parties involved, including auditors and other independent observers, and will also provide notification of any scheduled changes by April 15, 2025.

6. Encrypt all backup data-at-rest at the Agency's alternate site by November 30, 2024.

We consider management's planned corrective actions responsive to our recommendations. FHFA's written response, in its entirety, is included as Appendix II of this report.

APPENDIX I: METHODOLOGY

To accomplish our objective, we performed the following procedures:

- Reviewed General Accountability Office's *Standards for Internal Control in the Federal Government*. Determined that the design control and implement control activities component was significant to this objective. We focused on the underlying principles that management should: (1) design control activities to achieve objectives and respond to risks; (2) continue to evaluate changes in the use of information technology, design new control activities when these changes are incorporated into the entity's information technology infrastructure, and design control activities needed to maintain the information technology infrastructure, which often includes backup and recovery procedures, as well as continuity of operations plans, depending on the risks and consequences of a full or partial power systems outage; and (3) implement control activities through policies.
- Reviewed the following NIST publications and other federal guidelines:
  - NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Federal Information Systems and Organizations* (updated December 10, 2020)
  - NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems* (November 11, 2010)
  - NIST Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* (March 2006)
  - OMB Circular No. A-130, *Managing Information as a Strategic Resource* (July 28, 2016)
- Reviewed the following FHFA policies and procedures:
  - FHFA Common Control Plan (May 10, 2023)
  - FHFA Contingency Planning Standard, Rev. 2.1 (November 30, 2022)
  - Disaster Recovery Procedures for FHFA Production Systems OTIM-550, Version 5.4 (November 1, 2023)
  - OTIM Business Impact Analysis Report (May 2022)

- Reviewed and analyzed FHFA's contingency planning documents and policies to determine if FHFA effectively planned and maintained the GSS Contingency Plan in accordance with NIST and FHFA standards.

- Reviewed FY2024 IG FISMA Reporting Metrics 60 through 65 and assessed FHFA's maturity level through our analysis of FHFA's contingency planning documentation and our observations of FHFA's DREs to determine the effectiveness of FHFA's contingency planning.

- Observed and analyzed FHFA's FY 2024 DRE on November 5, 2023, and March 22, 2024, to determine if FHFA successfully followed the test procedures in the recovery procedures as planned and documented the test results in accordance with NIST and FHFA standards. To perform our analysis, we took notes and screenshots during the test and followed up with the recovery team to clarify our observations. FHFA remotely conducted both parts of its DRE, which we observed virtually.

- Reviewed and analyzed FHFA's alternate storage site documentation to determine whether the site supported storage and retrieval of backup information, and whether backups were conducted, tested, and protected at storage locations. Visited the alternate storage site to verify the controls in place and interview onsite personnel.

- Interviewed officials, staff, and contractors of FHFA's OTIM regarding FHFA's policies, procedures, process, and practices for contingency planning.

We conducted this performance audit from October 2023 to September 2024 in accordance with 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX II: FHFA MANAGEMENT RESPONSE.....

This page intentionally blank. See the following page(s).

Federal Housing Finance Agency

MEMORANDUM

TO: James Hodge, Deputy Inspector General for Audits

THROUGH: Katrina D. Jones, Chief Operating Officer

KATRINA JONES Digitally signed by KATRINA JONES Date: 2024.09.10 15:15:30 -04'00'

FROM: Luis Campudoni, Chief Information Officer

LUIS CAMPUDONI Digitally signed by LUIS CAMPUDONI Date: 2024.09.10 14:37:44 -04'00'

SUBJECT: Draft Audit Report: FHFA's Disaster Recovery Exercise for Its General Support System Needs Improvement

DATE: September 10, 2024

Thank you for the opportunity to respond to the above-referenced draft audit report (Report) by the Office of Inspector General (OIG), which contains 6 recommendations. As FHFA's new Chief Information Officer, I am pleased to respond to this report and to address the recommendations OIG has provided.

Recommendation 1: *Update the BIA annually in accordance with FHFA standards.*

Management Response for Recommendation 1: FHFA agrees with the recommendation and will update the Business Impact Analysis (BIA) by October 31, 2024.

Recommendation *2. Update the disaster recovery procedures document to ensure it includes (a) up to date time periods for the recovery time objective and the recovery point objective for resumption of the GSS operations consistent with the BIA, (b) database procedures, and (c) steps to validate successful failover and failback of the remote access infrastructure system.*

Management Response for Recommendation 2: FHFA agrees with the recommendations and will perform this action by April 15, 2025:

Update the disaster recovery procedures document to ensure it includes:

- Up-to-date periods for the recovery time objective and the recovery point objective for resumption of the General Support Systems operations consistent with the Business Impact Analysis,
- Database procedures, and
- Steps to validate successful failover and failback of the remote access infrastructure system.

Recommendation *3. Ensure the After Action Report is consistent with the Recovery Exercise Test Results by documenting all actions taken during the failover and failback of the DRE including all correct dates for when testing was conducted.*

Management Response for Recommendation 3: FHFA agrees with the recommendations. By April 15, 2025, FHFA will ensure the After-Action Report accurately captures the Disaster Recovery Exercise Test Results by documenting all actions taken during the failover and failback activities.

Recommendation *4. Perform annual testing of the contingency plan in accordance with the recovery procedures document to ensure failover and failback are conducted as planned.*

Management Response for Recommendation 4: FHFA agrees with the recommendation. By April 15, 2025, FHFA will perform annual testing of the contingency plan per FHFA's disaster recovery procedures and ensure failover and failback activities are conducted as planned.

Recommendation *5. Ensure OTIM officials communicate planned DREs and any scheduled changes with all parties involved, including auditors and other independent observers.*

Management Response for Recommendation 5: FHFA agrees with the recommendation. By April 15, 2025, OTIM officials will communicate the next planned Disaster Recovery Exercises to all parties involved, including auditors and other independent observers, and will also provide notification of any scheduled changes.

Recommendation *6. Encrypt all backup data-at-rest at FHFA's alternate site and update the existing POA&M to include compensating controls until the POA&M has been closed.*

Management Response for Recommendation 6: FHFA agrees with the recommendations. By November 30, 2024, FHFA will encrypt all backup data-at-rest at the Agency's alternate site.

cc: Edom Aweke
Tom Leach
Jeff Harris
Ralph Mosios
John Major
Warren Hammonds

Federal Housing Finance Agency
Office of Inspector General

To report potential fraud, waste, abuse, mismanagement, or any other kind of criminal or noncriminal misconduct relative to FHFA's programs or operations:

- Call: 1-800-793-7724
- Fax: 202-318-0358
- Visit: www.fhfaoig.gov/ReportFraud
- Write: FHFA Office of Inspector General
  Attn: Office of Investigations – Hotline
  400 Seventh Street SW
  Washington, DC 20219