Federal Housing Finance Agency
Office of Inspector General

FHFA's 2019 Disaster Recovery Exercise of its General Support System Was Conducted as Planned, But its Disaster Recovery Procedures Were Missing Certain Required Elements and Included Outdated Information

Audit Report • AUD-2020-005 • March 23, 2020

AUD-2020-005

March 23, 2020

Executive Summary

The Federal Housing Finance Agency (FHFA or Agency), established by the Housing and Economic Recovery Act of 2008, is responsible for the supervision, regulation, and housing mission oversight of Fannie Mae, Freddie Mac, and the Federal Home Loan Bank System.

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 to ensure the availability of critical information resources and continuity of operations in emergency situations. Agencies must also periodically test and evaluate their information security policies, procedures, and practices.

We performed this audit to determine whether FHFA conducted its 2019 Disaster Recovery Exercise (DRE) in accordance with its disaster recovery plan and procedures for recovering its General Support System (GSS). As part of our audit, we observed the DRE that took place in November 2019 and the physical security controls at FHFA's alternate operating facility in January 2020, and reviewed documentation related to the DRE. Additionally, we compared FHFA's contingency planning policies and procedures to NIST guidance.

We found that the GSS services identified for testing were tested as planned, and the tests were successful. We also determined that FHFA's internal reporting of the test results was reliable. However, we found that FHFA's disaster recovery procedures for the GSS were missing certain required elements and included outdated information, which creates the risk that an effective and timely recovery following a service disruption or real disaster may not occur.

We make two recommendations to address the identified shortcomings in this report. In a written management response, FHFA agreed with our recommendations.

This report was prepared by Jackie Dang, IT Audit Director, and Nick Peppers, Auditor-in-Charge; with assistance from Bob Taylor, Senior Advisor. 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.

Marla A. Freedman, Deputy Inspector General for Audits /s/

TABLE OF CONTENTS

ABBREVIATIONS

BIA	Business Impact Analysis
DR	Disaster Recovery
DRE	Disaster Recovery Exercise
DRP	Disaster Recovery Procedures
FHFA or Agency	Federal Housing Finance Agency
FISMA	Federal Information Security Modernization Act of 2014
GSS	General Support System
ISCP	Information System Contingency Plan
IT	Information Technology
MTD	Maximum Tolerable Downtime
NIST	National Institute of Standards and Technology
NIST 800-34	NIST SP 800-34, Rev. 1, Special Publication, Revision 1, *Contingency Planning Guide for Federal Information Systems*
OTIM	Office of Technology and Information Management
RTO	Recovery Time Objective
RPO	Recovery Point Objective
VoIP	Voice over Internet Protocol

BACKGROUND

Standards for Contingency Planning Controls and Testing

FISMA requires agencies, including FHFA, to develop, document, and implement agency-wide information programs to provide information security for the information and information systems that support the operations and assets of the agency. In addition, FISMA requires agencies to perform periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices. Testing shall include testing of management, operational, and technical controls of every information system identified in the agency's inventory. Pursuant to FISMA, NIST is responsible for developing standards and guidelines, including minimum requirements for federal information systems.

According to NIST's Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations. NIST Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* (NIST 800-34), 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.

Development of System Recovery Objectives

According to NIST, effective contingency planning begins with an agency's development of an organization contingency planning policy and a business impact analysis (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. For example, BIAs are used to determine things like:

- Maximum Tolerable Downtime (MTD) – the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption.

- Recovery Time Objective (RTO) – the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Because the

RTO must ensure that the MTD is not exceeded, the RTO is normally shorter than the MTD.

- Recovery Point Objective (RPO) – the point in time, prior to a disruption or system outage, to which mission/business process data must be recovered (given the most recent backup copy of the data) after an outage. RPO is a factor of how much data loss the mission/business process can tolerate during the recovery process.

Information System Contingency Plan Testing, Training, and Exercises

Required by NIST, an Information System Contingency Plan (ISCP) provides procedures for the assessment and recovery of a system following a system disruption. The ISCP provides key information needed for system recovery, including defining roles and responsibilities and identifying inventory information, assessment procedures, and detailed recovery procedures. An ISCP can be activated at the system's location or at an alternate site. NIST also requires that an ISCP should be maintained in a state of readiness, which includes having personnel trained to fulfill their roles and responsibilities, having plans exercised to validate their content, and having systems and system components tested to ensure their operability in the environment specified in the ISCP.

ISCP testing is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed by validating one or more of the system components and the operability of the plan. Among other things, NIST 800-34 states that contingency plan tests should include the following: notification procedures, system recovery on an alternate platform from backup media, internal and external connectivity, system performance using alternate equipment, and restoration of normal operations.

FHFA's General Support System

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 General Support System (GSS) is a wide area network that provides connectivity, information sharing and data processing capabilities, remote and network access, and security and support services.

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.

Contingency Planning Standard

FHFA's Contingency Planning Standard, Revision 1.3, defines the security requirements that FHFA information systems must have in supporting contingency planning capabilities. The standard calls for FHFA to:

- Maintain plan(s) outlining the resumption of essential mission and business functions in accordance with NIST 800-34;
- 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;
- Provide contingency training to Agency users consistent with assigned roles and responsibilities within the first year of assuming a contingency role or responsibility, when required by Agency system changes, and annually thereafter;
- Test the contingency plans at least annually, using table-top exercises and/or functional exercises to determine the effectiveness of the plans and the organizational readiness to execute the plans;
- Establish an alternate processing storage site to support the storage and retrieval of backup information;
- Establish alternate telecommunications services to permit the resumption of essential business functions based on the appropriate business impact analysis;
- Conduct backups of user-level information, system-level information, security-related documentation, and verify the integrity of backup information, as applicable, through contingency plan testing activities; and
- Protect the confidentiality, integrity, and availability of backup information at storage locations.

Disaster Recovery Procedures

FHFA's Disaster Recovery Procedures for FHFA Production Systems, Version 4.2 (November 1, 2019) (hereafter referred to as the DRP) constitutes the ISCP for the GSS and provides procedures for recovering a number of GSS critical IT services. The DRP assigns 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 (DR) Coordinator within

OTIM, in conjunction with OTIM's leadership. The DRP also provides for failover[1] and failback[2] procedures for critical GSS services and FHFA's public website.

FHFA's November 2019 Disaster Recovery Exercise

Historically, OTIM has conducted its DRE annually to validate the proper operation of the resiliency and recovery measures incorporated in FHFA's overall IT infrastructure. According to FHFA, these measures ensure the restoration of the production computing environment within an acceptable period of time in the event of an incident or disaster that disrupts normal computer operations.

For its November 2019 DRE, OTIM identified 10 of 13 critical GSS services to failover and failback during the period from November 2, 2019, to November 11, 2019. The DRE was timed to coincide with a scheduled building-wide power outage that was to occur on November 8, 2019, at 10 p.m. to November 10, 2019, at 4 p.m. In planning for the November 2019 DRE, the DR Coordinator created a "DR Failover Tracking Spreadsheet" to track critical DRE assignments, tasks, and/or events, such as identifying teams and individual assignments for various tasks, procedures for restoration, and team and end user communication. After the DRE was completed, as part of the procedures, OTIM prepared two documents:

- General Support Services Contingency Planning: 2020 DR Exercise Test Results dated December 3, 2019, which identified the tests conducted and included screen prints evidencing completion of the tests.
- OTIM After Action Report (undated), which discussed major strengths identified during this exercise as well as lessons learned. Examples of major strengths identified were successful failovers of all file shares and communications and the ability of the OTIM engineering team to perform restorative operations and deal with unexpected problems while geographically dispersed and operating remotely. According to the report, of the eight issues that occurred, all were resolved during the DRE period except for an issue with certain outdated audio-visual equipment.

[1] 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.

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

FACTS AND ANALYSIS

We observed FHFA's November 2019 DRE to assess whether it was conducted in accordance with its plan, as defined by its DR Failover Tracking Spreadsheet for recovering critical GSS services.

FHFA's November 2019 Disaster Recovery Exercise Tracked to its DR Failover Tracking Spreadsheet

Based on our observations and review of FHFA documentation, we found that the GSS services identified for testing in its DR Failover Tracking Spreadsheet were tested as planned. The failover and failback of the 10 tested GSS services were successful. We also determined that the reporting of the test results in the two documents, the General Support Services Contingency Planning: 2020 DR Exercise Test Results v.1 and the FHFA OTIM After Action Report/Improvement Plan Annual Disaster Recovery Exercise, was reliable.

Contingency Planning Procedures Were Missing Required Elements and Included Outdated Information

NIST 800-34 provides guidelines for preparing and maintaining ISCPs, discusses essential contingency plan elements and processes, highlights specific considerations and concerns associated with contingency planning for various types of information system platforms, and provides examples to assist the development of ISCPs. According to NIST, all ISCPs should be reviewed and tested at the frequency set by the organization (e.g., annually) or whenever there is a significant change to the system. Among other things, NIST requires the ISCP to include the following elements: the RTO, the RPO, equipment needed, vendor names, emergency contact, network diagram, and roles and responsibilities.

Among other things, NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* requires agencies to develop a contingency plan of the information system that provides recovery objectives, restoration priorities, and metrics; and an alternate processing site permits the transfer and resumption of the information system operations within defined time periods consistent with its RTO and RPO. Further, as documented in System Security Plan for General Support System (GSS), FHFA requires that "the GSS contingency plan define the time periods for achieving the recovery time objectives within which processing must be resumed at the alternate processing site."

We found that FHFA's DRP, which constitutes the ISCP for the GSS, was missing required elements and included outdated information. Accordingly, its DRP was not in a state of readiness required by NIST. For example:

- The DRP did not include the time periods for the RTO and RPO for resumption of GSS operation;
- The DRP did not include the procedures used to test for the failover and failback of FHFA's Voice over Internet Protocol (VoIP). Even so, we noted that the VoIP failover and failback were successfully tested during the November 2019 DRE;
- The DRP lacked lists of equipment needs, vendor names, and emergency contact information;
- Network diagrams in the DRP referenced the location of FHFA's former alternate operating facility instead of the location of its current alternate operating facility; and
- The individuals and titles listed under assigned roles and responsibilities in the DRP were outdated.

FINDING

FHFA's Disaster Recovery Procedures for the GSS Were Missing Certain Required Elements and Included Outdated Information

Our review of FHFA's GSS DRP found that certain required NIST elements, such as the time periods for the RTO and RPO, procedures used to test for the failover and failback of VoIP, lists of equipment needs, vendor names, and emergency contact information, were missing. The GSS DRP also included outdated information about FHFA's alternate operating facility and assigned roles and responsibilities. As a result, the GSS DRP was not in a state of readiness and creates the risk that an effective and timely recovery following a service disruption or real disaster may not occur.

CONCLUSION

FHFA conducted the 2019 DRE in accordance with its disaster recovery plan and procedures for recovering GSS services as planned, and the tests were successful. However, FHFA should address gaps and outdated information in its GSS DRP so that the procedures are in a ready state. The current unready state of the GSS DRP creates the risk that an effective and timely recovery following a service disruption or real disaster may not occur.

RECOMMENDATIONS

We recommend that FHFA

1. Update its GSS DRP to ensure the procedures include all NIST-required information and is in a ready state. In this regard, the procedures should provide time periods for the RTO and RPO for resumption of GSS operation; procedures used to test for the failover and failback of FHFA's VoIP; lists of equipment needs, vendor names, and emergency contact information; current information on FHFA's alternate operating facility; and current information on individuals and titles listed under assigned roles and responsibilities.

2. Maintain the GSS DRP in a ready state going forward.

FHFA COMMENTS AND OIG RESPONSE

We provided FHFA an opportunity to respond to a draft of this audit report. In its management response, which is included in the Appendix to this report, FHFA agreed with our two recommendations. As corrective actions, FHFA plans to:

1. Update the GSS DRP by October 31, 2020, to include RTO and RPO for resumption of GSS operation; procedures used to test for the failover and failback of FHFA's VoIP; lists of equipment needs, vendor names, and emergency contact information; current information on FHFA's alternate operating facility; and current information on individuals and titles listed under assigned roles and responsibilities.

2. Maintain the GSS DRP in a ready state by updating the DRP whenever there is a significant change in the GSS and, as necessary, through periodic reviews.

We consider FHFA's planned corrective actions responsive to our recommendations.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this audit was to determine whether FHFA conducted the 2019 DRE in accordance with its disaster recovery plan and procedures for recovering GSS services as planned for the DRE. As part of our audit, we observed the disaster recovery exercise that took place in November 2019 and physical security controls at the alternate site in January 2020.

The scope of this audit included a review of planning documentation related to the GSS as well as observation of the DRE in November 2019. We also reviewed the After-Action Report and documentation reporting the results of the DRE. Additionally, we reviewed adherence to applicable criteria including NIST and FHFA policies to determine if the disaster recovery capability was in place and had been successfully tested.

We also visited the alternate processing site. As part of the assessment, we observed physical security measures at the alternate site, such as fencing, locks, security guards, and badges. Additionally, we observed the structural and environmental measures of the storage facility, such as temperature, humidity, fire prevention, and power management controls.

We conducted this performance audit between November 2019 and March 2020 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: FHFA MANAGEMENT RESPONSE.....

Federal Housing Finance Agency

MEMORANDUM

TO: Marla Freedman, Deputy Inspector General for Audits

FROM: R. Kevin Winkler, Chief Information Officer CMS for RKW

SUBJECT: Draft Audit Report: *FHFA's 2019 Disaster Recovery Exercise of its General Support System Was Conducted as Planned; But its Disaster Recovery Procedures Were Missing Certain Required Elements and Included Outdated Information*

DATE: March 18, 2020

Thank you for the opportunity to respond to the above-referenced draft audit report by the Office of Inspector General (OIG). This memorandum provides the Federal Housing Finance Agency's (FHFA) management response to the two recommendations contained in the OIG's draft audit report. I am pleased that the audit concluded that the disaster recovery test was performed as planned; the failover and fallback of the tested services were successful; and the reporting of the test results was reliable. The responses to OIG's recommendations are below.

***Recommendation 1**: Update its GSS DRP to ensure the procedures include all NIST-required information and is in a ready state. In this regard, the procedures should provide time periods for the RTO and RPO for resumption of GSS operation; procedures used to test for the failover and failback of FHFA's VoIP; lists of equipment needs, vendor names, and emergency contact information; current information on FHFA's alternate operating facility; and current information on individuals and titles listed under assigned roles and responsibilities.*

Management Response: FHFA agrees with the recommendation and will update the Disaster Recovery Plan by October 31, 2020 to include Recovery Time Objective and Recovery Point Objective for resumption of GSS operation; procedures used to test for the failover and failback of FHFA's VoIP; lists of equipment needs, vendor names, and emergency contact information; current information on FHFA's alternate operating facility; and current information on individuals and titles listed under assigned roles and responsibilities.

Recommendation 2: *Maintain the GSS DRP in a ready state going forward.*

Management Response: FHFA agrees with the recommendation and will maintain the GSS DRP in a ready state by updating the DRP whenever there is a significant change in the GSS and, as necessary, through periodic reviews. OTIM will commit to update the DRP by October 31, 2020.

If you have any questions, please feel free to contact Stuart Levy at (202) 649-3610 or e-mail, Stuart.Levy@fhfa.gov.

CC: Chris Bosland
Larry Stauffer
T. Leach
J. Major
R. Mosios
C. Sherman
J. Vercellone
E. Hall

ADDITIONAL INFORMATION AND COPIES.....

For additional copies of this report:

- Call: 202-730-0880
- Fax: 202-318-0239
- Visit: www.fhfaoig.gov

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