Federal Housing Finance Agency
Office of Inspector General

FHFA Did Not Follow All of its Contingency Planning Requirements for the National Mortgage Database (NMDB) or its Correspondence Tracking System (CTS)

Audit Report • AUD-2022-003 • December 13, 2021

AUD-2022-003

December 13, 2021

Executive Summary

The Federal Housing Finance Agency (FHFA or Agency) is charged by the Housing and Economic Recovery Act of 2008 with the supervision of Fannie Mae and Freddie Mac (together, the Enterprises); Common Securitization Solutions, LLC (an affiliate of the Enterprises); the Federal Home Loan Banks (collectively, the regulated entities); and the Federal Home Loan Banks' fiscal agent, the Office of Finance. FHFA's mission as a federal financial regulator includes ensuring the safety and soundness of its regulated entities so that they serve as a reliable source of liquidity and funding for housing finance and community investment. Since 2008, FHFA has also served as conservator of the Enterprises.

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 conducted this audit to determine whether FHFA followed its standard for contingency planning controls for National Mortgage Database (NMDB) and the Correspondence Tracking System (CTS). The review period was October 1, 2019, through March 31, 2021 (review period).

We found that, as required, FHFA developed a contingency plan for NMDB. FHFA also conducted backups for NMDB and CTS at alternate storage locations. However, FHFA did not review or test the NMDB contingency plan annually. Further, although FHFA maintained that CTS "inherits" the contingency plan for FHFA's general support system (GSS) to meet its contingency plan requirements, we found that FHFA's GSS contingency plan did not make any reference to CTS or its servers, and the annual GSS contingency plan testing that FHFA did perform did not include CTS or its servers.

We make three recommendations in this report. In a written mangement response, FHFA agreed with our recommendations.

This report was prepared by Jackie Dang, Audit Director; Dan Jensen, Auditor-in-Charge; and David Peppers, IT Specialist; with assistance from Abdil Salah, Assistant Inspector General for Audits; James Hodge, Deputy Assistant Inspector General for Audits; and Bob Taylor, Senior Advisor. We

AUD-2022-003

December 13, 2021

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, Senior Audit Executive /s/

TABLE OF CONTENTS

ABBREVIATIONS

BIA	Business Impact Analysis
CTS	Correspondence Tracking System
Enterprises	Fannie Mae and Freddie Mac
FHFA or Agency	Federal Housing Finance Agency
FISMA	Federal Information Security Modernization Act of 2014
GSS	General Support System
IT	Information Technology
NIST	National Institute of Standards and Technology
NMDB	National Mortgage Database
OTIM	Office of Technology and Information Management
Regulated Entities	Fannie Mae, Freddie Mac, and the Federal Home Loan Bank System
SP	Special Publication

BACKGROUND

FHFA's Network 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. The National Mortgage Database (NMDB) is a comprehensive database of loan-level information about first lien single-family mortgages and for all individuals associated with a first lien single-family mortgage in NMDB, their credit line information.[1] The Correspondence Tracking System (CTS) captures and tracks correspondence that FHFA receives from external sources (e.g., the public, Congress, and the regulated entities). FHFA's general support system (GSS) is a wide area network that provides connectivity, information sharing and data processing capabilities, remote access, and security and support services for all FHFA information systems, including NMDB and CTS.

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. OTIM is responsible for GSS contingency planning controls, upon which NMDB and CTS rely.

Federal Standards for Contingency Planning Controls and Testing

The Federal Information Security Modernization Act of 2014 (FISMA) requires agencies, including FHFA, to develop, document, and implement agency-wide information programs to provide information security for the information and 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 their information security policies, procedures, and practices. Testing should include management, operational, and technical controls of every information system identified in the agency's inventory. Pursuant to FISMA, the National Institute of Standards and Technology (NIST) is responsible for developing standards and guidelines, including minimum requirements for federal information systems. In addition, NIST issues Special Publications (SP) as recommendation and guidance documents.

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

[1] According to FHFA's System Security Plan for NMDB, "No information on borrower names, addresses, Social Security numbers, or dates of birth is ever used or stored as part of the NMDB. Furthermore, safeguards are in place to ensure that information in the database is not used to identify individual borrowers or lenders and is handled in full accordance with federal privacy laws and the Fair Credit Reporting Act (FCRA)."

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 SP 800-34, Revision 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. NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, provides a catalog of security and privacy controls, including controls specifically related to contingency planning. Taken together, for contingency planning, NIST requires organizations to:

- Establish a contingency planning policy and procedure
- Develop and periodically update the contingency plan for each information system
- Provide contingency training for individuals consistent with their roles and responsibilities
- Test the contingency plan on a defined frequency
- Establish an alternate storage and processing site
- Perform information system backups
- Test for reliability and integrity of backups on a defined frequency

Development of System Recovery Objectives

According to NIST SP 800-34, effective contingency planning begins with an agency's development of a contingency planning policy for the organization and a business impact analysis (BIA) for each information system. The purpose of a BIA is to correlate the information system with the critical mission and service(s) it provides and, based on that information, characterize the consequences of a disruption. Using the BIA, agencies determine their contingency planning requirements and priorities. Analyzing the mission or business processes allows stakeholders to determine an acceptable downtime if a given process or system is disrupted or otherwise unavailable.

FHFA's Standard for Contingency Planning

Consistent with NIST requirements, FHFA's contingency planning standard defines the security requirements that FHFA information systems must have in support of 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 SP 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 BIA
- Conduct backups of user-level information, system-level information, and security-related documentation
- Protect the confidentiality, integrity, and availability of backup information at storage locations

FACTS AND ANALYSIS

As Required, FHFA Developed a Contingency Plan for NMDB and Conducted Backups for NMDB and CTS at Alternate Storage Locations

As required by its contingency planning standard, we found that FHFA:

- Developed a contingency plan that outlines the resumption of essential mission and business functions provided by NMDB
- Conducted backups of information and protected the confidentiality, integrity, and availability of backups for NMDB and CTS at alternate storage locations

FHFA Did Not Follow All Requirements in Its Standard for Contingency Planning for NMDB and CTS

For NMDB, we found that FHFA did not adhere to the following requirements in its contingency planning standard:

- The NMDB contingency plan had not been updated annually; this 13-page document was last updated May 2019
- FHFA did not test any aspect of the NMDB contingency plan in 2020 or 2021, as of March 31, 2021

For CTS, according to its February 2020 system security plan,[2] the system "inherits" the contingency plan for the GSS to meet its contingency plan requirements. However, our review of the GSS contingency plan found no references to CTS or its servers. Further, although FHFA performed tests of the GSS contingency plan annually, we found no evidence that testing included CTS or its servers.

OTIM officials cited lack of resources (inability to test everything) as the reason for the above shortcomings. Subsequent to the circulation of a draft of this report for technical comment, OTIM staff informed us that requests had been made for additional resources for the information security group responsible for updating and testing contingency plans, but those requests had been denied. We did not validate OTIM's assertion as part of this audit.

We note that from March 12, 2020, through the end of our review period, FHFA was working in a maximum telework status due to the COVID-19 pandemic. For NMDB and CTS, we found that FHFA demonstrated its ability to successfully operate both systems remotely for an extended period. However, the lack of an annual review and testing of the NMDB contingency plan increases the risk that the system may not be recovered successfully or timely in the event of a disruption.[3] Additionally, with the lack of a standalone contingency plan for CTS, or a clear reference to CTS and its servers in the GSS contingency plan and testing of that plan, FHFA has not assured the system could be recovered successfully or timely in the event of a disruption.

[2] NIST defines a system security plan as a formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

[3] NIST defines a disruption as an unplanned event that causes an information system to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

FINDINGS

- We found that FHFA developed a contingency plan for NMDB and conducted backups for NMDB and CTS at alternate storage locations. However, FHFA did not review or test the NMDB contingency plan annually, as required by its standard.
- We found that FHFA's GSS contingency plan did not make any reference to CTS or its servers, and when the annual GSS contingency plan testing was performed, it did not include CTS or its servers.

CONCLUSIONS

By periodically reviewing and testing contingency plans, management is provided with a level of assurance that, in the event of a disruption, systems can be recovered within an established recovery time objective. We found that FHFA developed a contingency plan for NMDB, established an alternate storage location, and performed backups at the alternate storage location. However, FHFA did not review or test the NMDB contingency plan annually, as required by its standard. Further, FHFA's GSS contingency plan did not make any reference to CTS or its servers, and the annual GSS contingency plan testing did not include CTS or its servers.

RECOMMENDATIONS

We recommend that FHFA:

1. Perform the required annual review and testing of the NMDB contingency plan.
2. Update the GSS contingency plan to include CTS and its servers, and ensure CTS and its servers are included in the annual GSS contingency plan testing.
3. Assess whether OTIM has sufficient, qualified staff to complete required updates and testing of its contingency plans in accordance with FHFA's standard and NIST requirements, and address any resource constraints that have adversely affected OTIM's ability to carry out its contingency planning requirements.

FHFA COMMENTS AND OIG RESPONSE

We provided FHFA an opportunity to respond to a draft of this audit report. FHFA provided technical comments on the draft report and those comments were considered in finalizing this report. FHFA also provided a management response, which is included in the Appendix of this report. In its management response, FHFA agreed with our recommendations and included the following planned corrective actions:

1. FHFA will complete an annual review and test the NMDB contingency plan by December 1, 2022.

2. FHFA will modify the GSS contingency plan to include CTS and its servers, and will include CTS and its servers in the next annual GSS contingency plan test by December 1, 2022.

3. OTIM will request an assessment to be completed by December 1, 2022, and that assessment will be used to determine if OTIM has sufficient resources (staff, technology, etc.) to update, test, and execute the contingency plan requirements.

In a meeting, an FHFA official clarified the Agency's response to recommendation 3. The official informed us that he expects the results of an independent third-party assessment will inform FHFA's actions going forward where possible and practical, including the formulation of the fiscal year 2024 budget request for resources.

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 followed its standard for contingency planning controls for NMDB and CTS. Our review period was October 1, 2019, through March 31, 2021.

We excluded from the scope of this audit report FHFA's compliance with requirements for contingency planning training because that requirement was assessed and reported on as part

of the fiscal year 2021 FISMA independent evaluation of FHFA's information security program and practices. That audit was performed by a contractor under our oversight.[4]

To accomplish our objective, we:

- Reviewed Government Accountability Office, *Standards for Internal Control in the Federal Government*, GAO-14-704G (September 2014), and determined that the control activities component of internal control was significant to this objective, along with the underlying principle, Principle 11, that management should design control activities to achieve objectives and respond to risks.

- Reviewed the following NIST publications:

  - NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* (May 2010, updated November 2010)

  - NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013, updated January 2015)

- We assessed the following FHFA policies, procedures, and guidance in effect during our review period and the extent to which these policies, procedures, and guidance were consistent with NIST requirements and the federal standards for internal control:

  - FHFA's contingency planning standard

  - Office of Technology and Information Management's business impact analysis report

  - The contingency plan for NMDB

  - The contingency plan for FHFA's GSS

- Reviewed and analyzed FHFA's contingency plans for NMDB and GSS, and determined whether the plans outlined the resumption of essential mission and business functions in accordance with the NIST publications cited above. Also determined whether the plans were reviewed and updated at least annually, or whenever a change to the operating environment or significant change to recovery procedures occurred. Our review of the GSS contingency plan was limited to the extent that it referenced CTS, as the system security plan for CTS stated that CTS

[4] The fiscal year 2021 FISMA audit found that FHFA did not provide contingency training to all Agency users with contingency related responsibilities. *See* OIG, *Audit of the Federal Housing Finance Agency's Information Security Program, Fiscal Year 2021* (Oct. 15, 2021) (AUD-2022-001) (online ***here***).

"inherited" the GSS contingency planning controls to meet its contingency plan requirements.

- Reviewed and analyzed NMDB and CTS contingency planning exercises to determine the effectiveness of the plans and organizational readiness to execute the plans.
- Reviewed and analyzed FHFA's alternate storage site(s) documentation to determine whether the site(s) supported storage and retrieval of backup information, and whether backups were conducted, tested, and protected at storage locations.
- 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 between April 2021 and December 2021 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 objective.

APPENDIX: FHFA MANAGEMENT RESPONSE.....

Federal Housing Finance Agency

MEMORANDUM

TO: Marla Freedman, Senior Audit Executive

THROUGH: Katrina D. Jones, Chief Operating Officer

FROM: Kevin Smith, Chief Information Officer KEVIN SMITH Digitally signed by KEVIN SMITH Date: 2021.11.30 09:38:44 -05'00'

SUBJECT: Draft Audit Report: *Draft Report for Management Comment - Audit of FHFA's Contingency Planning for NMDB and CTS*

DATE: November 30, 2021

Thank you for the opportunity to respond to the above-referenced draft audit report by the Office of Inspector General (OIG). This memorandum provides Federal Housing Finance Agency's (FHFA's) management response to the three recommendations contained in the draft report.

Recommendation 1: *Perform the required annual review and testing of the NMDB contingency plan.*

Management Response:

FHFA agrees with Recommendation 1 and will complete an annual review and test of the NMDB Contingency Plan by December 1, 2022.

Recommendation 2: *Update the GSS contingency plan to include CTS and its servers, and ensure CTS and its servers are included in the annual GSS contingency plan testing.*

Management Response: FHFA agrees with Recommendation 2 and will modify the GSS Contingency Plan to include CTS and its servers and will include CTS and its servers in the next annual GSS Contingency Plan test by December 1, 2022.

Recommendation 3: *Assess whether OTIM has sufficient, qualified staff to complete required updates and testing of its contingency plans in accordance with FHFA's standard and NIST requirements, and address any resource constraints that have adversely affected OTIM's ability to carry out its contingency planning requirements.*

Management Response: FHFA agrees with Recommendation 3. OTIM will request an assessment to be completed by December 1, 2022. The assessment will be used to determine if OTIM has sufficient resources (staff, technology, etc.) to update, test, and execute the contingency plan requirements.

If you have any questions, please contact Stuart Levy at (202) 689-9667 or e-mail, Stuart.Levy@fhfa.gov.

cc: Edom Aweke
Tom Leach
Tasha Cooper
Ralph Mosios
John Major

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