REDACTED

Federal Housing Finance Agency
Office of Inspector General

FHFA Took Actions to Ensure That Fannie Mae Adequately Addressed Deficiencies in Its Business Resiliency Program

This report contains redactions of information that is privileged or otherwise protected from disclosure under applicable law.

Evaluation Report • EVL-2024-001 • March 25, 2024

EVL-2024-001

March 25, 2024

Executive Summary

The Federal Housing Finance Agency (FHFA or Agency) defines business resiliency management for Fannie Mae and Freddie Mac (the Enterprises) as the "ability to minimize the impact of disruptions and maintain business operations at predefined levels." The Agency expects the Enterprises to establish and maintain a business resiliency program to respond to "[u]ncontrolled events, such as natural disasters, pandemics, and cyberattacks," which can threaten the regulated entities' ability to perform mission critical operations.

In 2021, we reported that FHFA found critical deficiencies in Fannie Mae's [redacted] practices and a lack of [redacted] during multiple examination cycles. FHFA agreed to complete a targeted examination of Fannie Mae's business resiliency during the 2022 examination cycle using "relevant criteria" in FHFA's advisory bulletin on business resiliency management. FHFA management stated that, based on these supervisory activities, it may issue adverse examination findings or enforcement actions, if warranted.

We conducted this evaluation to confirm that FHFA performed the examination activities it had committed to complete and to assess whether its supervisory efforts were successful in addressing the critical deficiencies in Fannie Mae's [redacted] program. Our evaluation verified that the Division of Enterprise Regulation (DER) completed several examination activities focused on Fannie Mae's business resiliency practices during the 2021 and 2022 examination cycles. We also verified that DER examiners assessed the Enterprise's practices against criteria from FHFA's advisory bulletin on business resiliency management. DER did not issue any matters requiring attention and concluded that Fannie Mae has [redacted].

Separate from DER's examination work, FHFA, as conservator, set objectives and prescribed specific business resiliency testing and reporting requirements for the Enterprises. FHFA exercised its authority as conservator and issued a Business Resiliency Directive in 2022 that highlighted the importance of the Enterprises developing recovery testing for their programs. The Directive requires each Enterprise to demonstrate its ability to switch to out-of-region locations, operate, and return to its normal information systems for each of its mission-critical applications. According to the Division of Conservatorship Oversight and Readiness (DCOR), Fannie Mae has met and continues to meet the requirements of the Directive, and its business resiliency program meets, and in some areas has exceeded, DCOR's expectations.

EVL-2024-001

March 25, 2024

We make no recommendations in this report.

We provided FHFA an opportunity to respond to a draft of this evaluation report. FHFA provided technical comments on the draft report, which were considered in finalizing this report.

This report was prepared by Adrienne Freeman, Attorney Advisor, and Jacob Kennedy, Senior Investigative Evaluator. 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.

/s/

Kyle D. Roberts
Deputy Inspector General for Evaluations

TABLE OF CONTENTS ....

ABBREVIATIONS

DCOR	Division of Conservatorship Oversight and Readiness
DER	Division of Enterprise Regulation
FHFA or Agency	Federal Housing Finance Agency
MRA	Matter Requiring Attention
OIG	Office of Inspector General
PMOS	Prudential Management and Operations Standards

BACKGROUND

FHFA Has Emphasized the Importance of Business Resiliency Management at the Enterprises

FHFA defines business resiliency management for the Enterprises as the "ability to minimize the impact of disruptions and maintain business operations at predefined levels."[1] FHFA has emphasized that the Enterprises must "maintain their focus on operational resiliency, to minimize the impact of operational disruptions and to ensure that mission-critical applications and processes can be recovered if they are impaired as a result of a significant operational incident."

FHFA expects the Enterprises to establish and maintain a business resiliency program to respond to "[u]ncontrolled events, such as natural disasters, pandemics, and cyberattacks," which can threaten the regulated entities' ability to perform mission critical operations. Should the Enterprises be unable to manage these risks, there could be an immediate impact on the mortgage finance industry, with disruptions having widespread impact on the financial services industry, homeowners, and investors.

FHFA Consistently Found Critical Deficiencies in Fannie Mae's [redacted] Program Over Multiple Examination Cycles

In 2021, we reported that FHFA found critical deficiencies in Fannie Mae's [redacted] practices and a lack of [redacted] during multiple examination cycles.[2] DER concluded in 2012 that "[redacted]" and FHFA issued a Matter Requiring Attention (MRA).[3] Notwithstanding these critical

---

[1] FHFA, Advisory Bulletin 2019-01, *Business Resiliency Management*, at 1 (May 7, 2019).

[2] For further discussion of the Enterprises' business resiliency program and risks, see OIG, *For Nine Years, FHFA Has Failed to Take Timely and Decisive Supervisory Action to Bring Fannie Mae into Compliance with its Prudential Standard to Ensure Business Resiliency* (Mar. 22, 2021) (EVL-2021-002).

[3] An adverse examination finding is an issue or deficiency related to risk management, risk exposure, or violations of laws, regulations, or orders affecting the performance or condition of a regulated entity. An MRA is one of the three categories of adverse examination findings. MRAs require remediation by an Enterprise's board of directors, management, or both. FHFA issues two types of MRAs, depending on the nature and severity of the findings and the priority for remediation: (1) critical supervisory matters (the highest priority) and (2) deficiencies. *See* FHFA, Advisory Bulletin 2017-01, *Classifications of Adverse Examination Findings* (Mar. 13, 2017).

deficiencies, at the time we issued our report, multiple examination cycles had passed and DER had not issued an MRA (a form of adverse examination finding) to prompt remediation.[4]

FHFA Agreed to Complete Examination Activities Pertaining to Business Resiliency During the 2022 Examination Cycle

In our report, we recommended that DER assess Fannie Mae's business resiliency practices and capabilities during the 2021 examination cycle (which was ongoing at that time) and "formally determine whether they meet or fail to meet [the applicable prudential management and operations standard]."[5] In its response, FHFA management agreed to complete a targeted examination of Fannie Mae's business resiliency during the 2022 examination cycle (i.e., the subsequent examination cycle) using "relevant criteria" in FHFA's advisory bulletin on business resiliency management.[6]

FHFA management also advised that examiners were monitoring Fannie Mae's business resiliency practices during the 2021 examination cycle. The then Deputy Director of DER advised us that, based on these supervisory activities, it may issue adverse examination findings or enforcement actions, if warranted.

After our report was published, DER adopted new guidance for examination processes and documentation standards. DER now instructs examiners to prepare a memorandum for each critical supervisory matter and to include, among other things, recommendations to pursue or not pursue an enforcement action for nonadherence with a relevant PMOS.

We conducted this evaluation to confirm that FHFA performed the examination activities it had committed to complete and to assess whether DER's supervisory efforts were successful in addressing the critical deficiencies in Fannie Mae's [redacted] program.

---

[4] Within FHFA, DER is responsible for supervising the Enterprises to ensure that they operate in a safe and sound manner. DER's supervisory program includes targeted examinations, ongoing monitoring, and risk assessments. *See* FHFA, Supervision & Regulation.

[5] Our report identified the applicable prudential standard as Standard 8, Principle 11, from FHFA's prudential management and operations standards (PMOS). Principle 11 states that "a regulated entity should have adequate and well-tested disaster recovery and business resumption plans for all major systems and have remote facilitates [sic] to limit the effects of disruptive events." The PMOS are FHFA's minimum standards for the risk management practices of the Enterprises (and the Federal Home Loan Banks and the Office of Finance), and the FHFA Director has a statutory duty to ensure that each of those regulated entities complies with the PMOS. The PMOS are found at 12 C.F.R. Part 1236, Appendix A (amendment published at 89 FR 3539, Jan. 19, 2024).

[6] FHFA's Advisory Bulletin 2019-01 communicates the Agency's supervisory guidance and the relevant criteria. In particular, it states that priority-based testing should "include a full-scale [disaster recovery] test to confirm the entity's ability to conduct and sustain normal business in an alternate data center and ability to return to pre-defined levels of operations in the primary data center."

FACTS AND ANALYSIS ....

DER Completed a Targeted Examination and Other Examination Activities of Fannie Mae's Business Resiliency Program

DER Conducted the Targeted Examination It Agreed to Conduct

We confirmed that DER examiners completed a targeted examination that assessed elements of Fannie Mae's business resiliency management program. The scope of the examination included governance, risk mitigation, and the testing program. DER examiners assessed Fannie Mae's practices against corresponding criteria in FHFA guidance on business resiliency management. Based on this examination work, DER did not identify supervisory concerns that rose to the level of an MRA. According to FHFA, Fannie Mae has [redacted].

DER Conducted Additional Examination Activities During the 2021 and 2022 Examination Cycles Pertaining to Fannie Mae's Business Resiliency Program

We confirmed that DER examiners conducted several other examination activities related to Fannie Mae's business resiliency practices during the 2021 and 2022 examination cycles; specifically, the examiners conducted two other targeted examinations and four ongoing monitoring activities.[7] The scope of those examination activities included assessing Fannie Mae's business recovery exercise test results, business continuity plans, business impact analysis, and key performance indicators.

DER did not identify supervisory concerns that rose to the level of an MRA.[8] At year-end 2022, DER characterized the quality of Fannie Mae's risk management of [redacted].

[7] As part of its ongoing monitoring activities, DER examiners review what Fannie Mae tests, how the Enterprise conducts its testing, its ability to meet the desired recovery times, and whether Fannie Mae took appropriate actions when recovery times were not met. They also meet bi-monthly with Fannie Mae management to discuss the Enterprise's business resiliency program testing. Further, the examiners told us they review the quarterly reports on testing and business resiliency that Fannie Mae submits in accordance with a directive issued by FHFA as conservator.

[8] FHFA has acknowledged that Fannie Mae's business resiliency program has made positive developments since our 2021 evaluation. For example, Fannie Mae has reported reduced testing recovery times. Whereas business resiliency practice at the time of our 2021 report focused on out-of-region data centers, Fannie Mae's current practice relies significantly on cloud computing as a solution for disaster recovery. According to FHFA, Fannie Mae's reliance on "the cloud" for disaster recovery has shifted the risk from out-of-region data centers to cloud resiliency. Cloud computing is a technology service that provides on-demand access to a shared pool of computing resources over the internet and enables flexible, scalable, and a broadly available computing infrastructure that is owned and maintained, typically off-site, by a cloud service provider.

FHFA, as Conservator, Set Objectives and Prescribed Specific Business Resiliency Testing and Reporting Requirements for the Enterprises

Separate from the examination work conducted by DER, FHFA set internal scorecard objectives in 2020 and 2021 for the Enterprises to develop their business resiliency programs and ensure that the Enterprises could recover from a disaster event. The scorecards included goals for the Enterprises to develop business resiliency plans and objectives, and to establish recovery times and recovery points for mission critical systems.[9]

A DCOR official explained that after the Enterprises had established business resiliency plans and programs, FHFA exercised its authority as conservator and issued a Business Resiliency Directive (the Directive) in 2022.[10] According to this official, the Directive highlighted the importance of the Enterprises developing recovery testing for their programs. He explained to us that the Directive would focus management's attention on testing and enable the Enterprises to address resiliency issues faster than they had been addressed in the past.

The Business Resiliency Directive Required the Enterprises to Demonstrate Their Disaster Recovery Abilities, Conduct Testing, and Report Testing Results to FHFA

The objective of the Directive is to "ensure that the Enterprises maintain their focus on operational resiliency, to minimize the impact of operational disruptions, and to ensure that mission-critical applications and processes can be recovered if they are impaired as a result of a significant operational incident." Among other things, the Directive requires each Enterprise to demonstrate its ability to switch to out-of-region locations, operate, and return to its normal information systems for each of its mission-critical applications.

The Enterprise must submit a quarterly plan that shows the out-of-region rotation (or testing) schedule, along with a report showing the cumulative results of any testing or rotation that has occurred during the calendar year. The reporting should indicate, among other things, the degree to which the switch or rotation exercise achieved its business recovery time objective for each mission-critical application.

According to a DCOR official, Fannie Mae has met and continues to meet the requirements of the Directive. Fannie Mae reports quarterly on this testing, and DCOR told us they review those reports to determine testing completion rates and identify any patterns and trends.

---

[9] The Directive defines mission critical as "the business processes, technology applications, and supporting infrastructure that are required to fulfill existing financial and contractual obligations and to support the orderly functioning of the primary and secondary mortgage markets (including but not limited to underwriting, committing, sale, delivery, servicing, and securitization)." Fannie Mae has reported that it has close to 500 mission critical applications and processes.

[10] Conservatorship directives from FHFA to the Enterprises set forth significant policy determinations by FHFA and provide specific direction to undertake separate or joint actions.

According to this official, Fannie Mae's business resiliency program meets, and in some areas has exceeded, DCOR's expectations.

Fannie Mae's Growing Reliance on the Cloud Increases Its Exposure to Risk from Third-Party Service Providers

FHFA staff informed us that the majority of Fannie Mae's applications – including mission critical applications – have migrated to the cloud, and a single third-party provider hosts the largest number of Fannie Mae's applications in the cloud. The increasing use of cloud computing exposes the Enterprise to additional concentration, operational, reputational, and information security risks that arise when applications are migrated to the cloud.[11] Indeed, FHFA's 2022 Annual Report to Congress described how its regulated entities rely on third-party providers and how that reliance can pose critical risk to its operations.[12]

FHFA's supervisory guidance on the oversight of third-party providers states that the more risk a third-party provider poses, the more rigorously the regulated entity should perform its risk management activities.[13] Both DER and DCOR told us they review Fannie Mae's testing procedures and results for cloud resiliency; however, unlike other federal financial safety and soundness supervisors, FHFA lacks express statutory authority to examine the third-party that provides this critical service. Presently, Fannie Mae's reliance on a third-party to host the majority of its mission-critical processes presents a significant exposure to third-party risk.

FHFA's supervisory and examination activities specific to third-party service providers and cloud computing were outside of the scope of this evaluation. OIG is planning future work in this area.

---

[11] For example, in 2021, Fannie Mae reported it experienced a [redacted]. At the time of the [redacted], Fannie Mae was unable to [redacted]. Fannie Mae initiated remediation efforts to address the lack of a [redacted] and its failure to meet 2021 resiliency requirements. In response to this [redacted], DER's 2022 examination activities included an assessment of the [redacted]. According to DER, all mission critical applications that have been migrated to the cloud have undergone disaster recovery testing.

[12] FHFA recommended that Congress authorize FHFA to examine the records, operations, and facilities of each material service provider to a regulated entity with regard to the services provided. The Agency stated, in pertinent part: "Were Congress to grant FHFA such authority, giving FHFA tailored parity with other federal financial regulators, the Agency would be in a better position to achieve its statutory duty to ensure the safe and sound operations of the Enterprises and FHLBanks." *See* FHFA, *2022 Report to Congress*.

[13] FHFA, Advisory Bulletin 2018-08, *Oversight of Third-Party Provider Relationships* (Sept. 28, 2018).

CONCLUSIONS

We conducted this evaluation to confirm that FHFA performed the examination activities it committed to conduct in response to our 2021 evaluation report and to assess whether DER's supervisory efforts were successful in addressing the critical deficiencies in Fannie Mae's [redacted] program. We make no recommendations in this report.

We verified that DER examiners conducted a 2022 targeted examination on business continuity in direct response to our 2021 evaluation. They also conducted ongoing monitoring activities that reviewed Fannie Mae's business resiliency testing during the relevant examination cycles. Based on this activity, DER did not identify supervisory concerns that rose to the level of an MRA and has concluded that Fannie Mae has [redacted].

Subsequent to our 2021 report, FHFA, as conservator, issued the 2022 Business Resiliency Directive. The Directive requires the Enterprise to conduct prescribed testing and to report the testing results to FHFA, and both DCOR and DER staff told us they review those results. Fannie Mae also adopted a business resiliency strategy that relies on a third-party cloud service provider to host most of the Enterprise's mission critical applications and processes. Fannie Mae's increased reliance on the provider, and FHFA's lack of express statutory authority to examine the provider, may be the subject of future OIG work.

OBJECTIVE, SCOPE, AND METHODOLOGY ....

We conducted this evaluation to confirm that FHFA performed the examination activities it had committed to complete in response to our 2021 evaluation and to assess whether DER's supervisory efforts were successful in addressing the critical deficiencies in Fannie Mae's [redacted] program and ensuring its disaster recovery capabilities meet the applicable prudential management and operations standards. After we issued our 2021 report, DER adopted new examination guidance. DER now instructs examiners to prepare a memorandum for each critical supervisory matter and to include, among other things, recommendations to pursue or not pursue an enforcement action for nonadherence with a relevant PMOS. The review period for this evaluation was from October 1, 2020, through September 30, 2023.

To meet this objective, we reviewed applicable FHFA guidance and standards in effect during our review period, including the applicable federal regulations, conservatorship directives, advisory bulletins, and operating procedures bulletins. We also reviewed prior OIG reports, Fannie Mae reports of examination, Fannie Mae board materials and risk assessments, Fannie Mae business resiliency quarterly plans and reporting, relevant DER examination workpapers, and other FHFA and Enterprise documents regarding Fannie Mae's business resiliency program.

As part of this evaluation, we conducted interviews of DCOR and DER staff involved in oversight of Fannie Mae's business resiliency program.

We provided FHFA an opportunity to respond to a draft of this evaluation report. FHFA provided technical comments on the draft report, which were considered in finalizing this report.

This evaluation was conducted between October 2023 and February 2024 under the authority of the Inspector General Act and in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* (December 2020).

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