REDACTED

Federal Housing Finance Agency
Office of Inspector General

FHFA Failed to Ensure Freddie Mac's Remedial Plans for a Cybersecurity MRA Addressed All Deficiencies; as Allowed by its Standard, FHFA Closed the MRA after Independently Determining the Enterprise Completed its Planned Remedial Actions

This report contains redactions of information that is privileged or confidential.

Audit Report • AUD-2018-008 • March 28, 2018

AUD-2018-008

March 28, 2018

Executive Summary

The Federal Housing Finance Agency (FHFA) is charged with ensuring that the Federal National Mortgage Association (Fannie Mae) and the Federal Home Loan Mortgage Corporation (Freddie Mac) (together, the Enterprises) operate in a safe and sound manner. Within FHFA, the Division of Enterprise Regulation (DER) is responsible for the supervision of the Enterprises.

Recognizing that consequences from any number of planned or unplanned scenarios may threaten an institution's ability to perform operations on any particular day, FHFA has established guidance in its *Examination Manual* for FHFA examiners to assess the sufficiency of [redacted] by the entities FHFA regulates, including the Enterprises. According to FHFA, an effective [redacted] is a risk mitigant. In the event of a disruption to an Enterprise's business, such as from a cyber attack, technology system upgrade, natural disaster, infrastructure failure, human error, or act of terrorism, an ineffective [redacted] may create "an inability to fulfill obligations and provide continuous services [which] may result in legal liability and tarnish the institution's reputation."

Based on a 2011 targeted examination of Freddie Mac's [redacted] and [redacted], DER concluded, among other things, that "[t]he safety and soundness of existing [redacted] and [redacted] programs present [redacted]. [redacted] means that business operations are [redacted], and the [redacted] are [redacted] and [redacted] and [redacted]. … The Enterprise cannot fully [redacted] most of its [redacted] during a [redacted] and cannot [redacted] even [redacted] for more than a few days."

In 2012, DER issued a Matter Requiring Attention (MRA) to Freddie Mac for its inadequate and ineffective [redacted]. DER instructed Freddie Mac to fully implement "an effective [redacted] program with adequate [redacted] provisions to ensure the preservation of the Enterprise in the [redacted] of [redacted] to [redacted]. … The program should be designed to prudently protect [redacted] from the effects of [redacted] and [redacted] and to ensure timely [redacted] of [redacted]. It should also provide for verifying and monitoring [redacted] programs and [redacted]."

When an MRA is issued, FHFA requires the Enterprise to provide a remedial plan, with specific milestones taking into consideration the complexity of the issue and the urgency regarding correction. From 2012 to 2014, Freddie Mac

submitted three remedial plans to DER to address this MRA. According to DER's guidance in effect at the time the MRA was issued, DER examiners were tasked with reviewing the proposed remedial plan to determine whether it was "sufficiently detailed and appropriate to resolve the MRAs."

This audit is a follow-on to our audit report *FHFA Did Not Complete All Planned Supervisory Activities Related to Cybersecurity Risks at Freddie Mac for the 2016 Examination Cycle* (AUD-2017-011) (September 27, 2017). In that audit, we found that for the 2016 examination cycle, DER completed four of the six cybersecurity-related supervisory activities it planned, one of which was an ongoing monitoring activity on Freddie Mac's efforts to remediate the above cybersecurity-related MRA. We are building upon our previous audit work to determine, for this MRA closed in 2016, whether FHFA examiners followed existing requirements in issuing "non-objection" letters to Freddie Mac's remedial plans and in independently verifying Freddie Mac's implementation of its remediation plans.

DER guidance in effect when Freddie Mac submitted two of its three remedial plans required examiners to determine whether the proposed plan would resolve the deficiency giving rise to the MRA and to issue a non-objection letter when an affirmative decision was made. Here, DER issued non-objection letters to the second and third remedial plans submitted by Freddie Mac (and issued no response to the first plan because none was required). We found, however, that the three remedial plans did not address all deficiencies identified with the MRA. Specifically, none of Freddie Mac's three remedial plans for this MRA, dated February 2012, August 2013, and November 2014, included any planned steps to [redacted] programs and [redacted].

DER's guidance in effect at the time this MRA was closed in May 2016 directed examiners to assess whether the remediation plan was implemented as intended and that the planned remediation is complete. We sought to determine whether DER followed its guidance in closing this MRA in May 2016. We examined whether DER independently assessed Freddie Mac's implementation of its remedial plans. We found that DER documented its review of evidence submitted by Freddie Mac to demonstrate that the corrective action items and/or milestones in the August 30, 2013, and November 12, 2014, remedial plans were met, including its review of [redacted], [redacted], [redacted] and [redacted], test plans, test results, and a contractor's report on the testing results. Accordingly, DER met its standard in its closure of this MRA. Because none of Freddie Mac's remedial plans addressed one of the

AUD-2018-008

March 28, 2018

critical defiencies identified in the MRA, DER had no evidence that this deficiency was remediated.

We make two recommendation(s) to FHFA to address the shortcomings identified in this audit. In a written management response, FHFA agreed with the recommendations. Its planned corrective actions are responsive to the recommendations.

We are also issuing today the results of our audit of FHFA's verification of Fannie Mae's remediation of three cybersecurity related MRAs during the 2016 examination cycle. See *As Allowed by its Standard, FHFA Closed Three Fannie Mae Cybersecurity MRAs after Independently Determining the Enterprise Completed its Planned Remedial Actions* (AUD-2018-007), online at www.fhfaoig.gov/reports/auditsandevaluations.

Key contributors to this report were: Jackie Dang, IT Audit Director; Terese Blanchard, Auditor-in-Charge; David Cho, IT Specialist; and Nick Peppers, IT Specialist; with the assistance of Bob Taylor, 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.

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

TABLE OF CONTENTS

ABBREVIATIONS

AB	Advisory Bulletin
DER	Division of Enterprise Regulation
Enterprises	Fannie Mae and Freddie Mac
Fannie Mae	Federal National Mortgage Association
FHFA or Agency	Federal Housing Finance Agency
Freddie Mac	Federal Home Loan Mortgage Corporation
MRA	Matter Requiring Attention
OIG	Federal Housing Finance Agency Office of Inspector General
[redacted]	[redacted]
OPB	Operating Procedures Bulletin
PIR	Pre-Implementation Review

BACKGROUND

Created by Congress in 2008, FHFA is charged by the Housing and Economic Recovery Act of 2008 with, among other things, the supervision of the Enterprises. Its mission as a federal financial regulator includes ensuring the safety and soundness of the regulated entities so that they serve as a reliable source of liquidity and funding for housing finance and community investment. FHFA exercises its supervision of the Enterprises through DER.

FHFA Emphasizes the Importance of [redacted] to Address Cyber Attacks and Other Threats

Recognizing that consequences from any number of planned or unplanned scenarios may threaten an institution's ability to perform operations on any particular day, FHFA has established guidance in its *Examination Manual* for FHFA examiners to assess the sufficiency of [redacted] by its regulated entities.[1] FHFA defines [redacted] as an organization's preparation process to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions even under extraordinary circumstances. According to FHFA, an effective [redacted] is a risk mitigant. In the event of a disruption to an Enterprise's business, such as from a cyber attack or event, technology system upgrade, natural disaster, infrastructure failure, human error, or act of terrorism, an ineffective [redacted] may create "an inability to fulfill obligations and provide continuous services [which] may result in legal liability and tarnish the institution's reputation."

In 2010, Freddie Mac's Internal Audit Function Identifies, as a Major Issue, Problems with the Enterprise's [redacted]

In September 2010, Freddie Mac's Internal Audit function (hereafter referred to as Internal Audit) issued a report that identified the [redacted] as a major issue:[2]

> Freddie Mac's operations are [redacted] in [redacted]…. The [redacted] strategy approved and implemented in 2009 … does not address processes required to [redacted] (e.g. [redacted]) which

[1] This guidance is set forth in the [redacted] module of the *FHFA Examination Manual* (online at www.fhfa.gov/SupervisionRegulation/ExaminerResources/Pages/Manual-and-Supplemental-Guidance.aspx) (accessed Feb. 7, 2018).

[2] Internal Audit defines a "major" issue as an issue that is reported to senior management and the board of directors. Internal Audit defines an "other" issue as an issue that is not considered as significant as a major issue; other issues are reported to upper management.

> increases the likelihood that the company may not [redacted] timely and [redacted] in case of [redacted] affecting [redacted].

DER Issued an MRA to Freddie Mac for its Inadequate and Ineffective [redacted] in January 2012

DER develops an annual supervisory strategy for each Enterprise and implements that strategy through an annual supervisory plan. The annual supervisory plan for each Enterprise sets forth the objectives for carrying out the supervisory strategy and identifies the supervisory activities, both targeted examinations and ongoing monitoring, for the year. During its supervisory activities, FHFA examiners may identify supervisory concerns or deficiencies and such examination findings are categorized as follows: (1) MRAs,[3] (2) violations, and (3) recommendations.

According to FHFA, only "the most serious supervisory matters" are categorized as MRAs. FHFA will issue an MRA for such matters as "non-compliance with laws or regulations that result or may result in significant risk of financial loss or damage to the regulated entity," "repeat deficiencies that have escalated due to insufficient action or attention," "unsafe or unsound practices," "matters that have resulted, or are likely to result, in a regulated entity being in an unsafe or unsound condition," and "breakdowns in risk management, significant control weaknesses, or inappropriate risk-taking."

Based on a 2011 targeted examination of Freddie Mac's [redacted] and [redacted], DER concluded, among other things, that:

> The safety and soundness of existing [redacted] and [redacted] programs present [redacted]. [redacted] means that business operations are [redacted], and the [redacted] are [redacted] and [redacted] and [redacted]. … The Enterprise cannot [redacted] most of its [redacted] during a [redacted] and cannot [redacted] even [redacted] for more than a few days.

In a letter dated January 27, 2012, DER issued an MRA to Freddie Mac for its inadequate and ineffective [redacted]. DER instructed Freddie Mac that it needed to fully implement:

---

[3] For the period covered by this audit, FHFA Advisory Bulletin (AB) AB 2012-01, *Categories for Examination Findings*, was in force. This AB was superseded and rescinded by AB 2017-01, *Classifications of Adverse Examination Findings* (Mar.13, 2017) (online at www.fhfa.gov/SupervisionRegulation/AdvisoryBulletins/Pages/Classifications-of-Adverse-Examination-Findings.aspx) (accessed Feb. 6, 2018).

> …an [redacted] program with adequate [redacted] provisions to ensure the [redacted] of the Enterprise in the [redacted] [redacted] to [redacted]. This should involve identifying, selecting, implementing, testing, reporting, and updating relevant policies, procedures, reports, and processes that meet the Enterprise's [redacted] and [redacted] objectives. The program should be designed to prudently protect [redacted] from the effects of [redacted] and [redacted] and to ensure [redacted] of [redacted]. It should also provide for verifying and monitoring [redacted] programs and [redacted].

The letter cited a "[redacted]" identified by Freddie Mac's Operational Risk Management function that needed to be addressed. Among the risks identified:

- "The Enterprise lacks a [redacted] program to develop, implement, and oversee the type of comprehensive Enterprise-wide and business-level [redacted], [redacted], and [redacted] commensurate with the needs of the Enterprise;"
- "Current [redacted] are not viable and do not meet the Enterprise's [redacted];" and
- "Existing [redacted] do not address cases in which a [redacted] is unable to [redacted] and/or [redacted]."

Freddie Mac Submitted an Initial and Two Amended Remedial Plans for this MRA

FHFA issues advisory bulletins (ABs) to FHFA supervision staff and the regulated entities on specific supervisory matters. In April 2012, FHFA issued AB 2012-01, *Categories for Examination Findings* (April 2, 2012). AB 2012-01 requires an Enterprise to respond to an MRA with a proposed written remedial plan, including specific milestones taking into consideration the complexity of the issue and the urgency regarding correction. From 2012 to 2014, Freddie Mac submitted three remedial plans to DER for this MRA. According to DER's internal guidance in effect as of April 2013 through May 2016, when this MRA was closed, DER examiners were tasked with reviewing the proposed remedial plan to determine whether it was "sufficiently detailed and appropriate to resolve the MRAs." When DER examiners concluded that the proposed plan would resolve the MRA, it would issue a non-objection letter to the Enterprise. Below is a brief description of the three plans:

- **Initial Remedial Plan**: On February 23, 2012, Freddie Mac submitted an initial remedial plan which established four initiatives to remediate the MRA by December 31, 2013, and to deliver a closure package by February 15, 2014. The four

initiatives were: (1) [redacted] (e.g., [redacted]), (2) [redacted] program, (3) [redacted] (e.g., [redacted]), and (4) [redacted] addressing [redacted]. Because DER guidance in effect at that time did not require DER issuance of a non-objection letter for a remedial plan, none was issued.[4]

- **Second Remedial Plan**: On August 30, 2013, Freddie Mac submitted a second plan to extend the targeted implementation date for the remaining action to September 30, 2014.[5] Freddie Mac reported that a more comprehensive technology solution had been developed to address its [redacted] and [redacted]. Freddie Mac also explained that one of the four initiatives in the initial remedial plan, "implementation of '[redacted] addressing [redacted]' required additional time to complete." DER issued a non-objection letter after review of this plan.

- **Third Remedial Plan**: Freddie Mac submitted a third plan, dated November 12, 2014, after the target implementation date established in the second plan had expired.

  This third plan was developed in response to a May 8, 2014, memorandum by Freddie Mac Internal Audit on the results from a "pre-implementation review" (PIR) of the Enterprise's testing approach for its [redacted] and [redacted] programs. Internal Audit stated in its memorandum that the "[redacted]" testing planned for 2014, which focused on [redacted], testing of the [redacted], and [redacted], was "not sufficient to provide reasonable assurance that the company can [redacted] based on a [redacted], as it does not sufficiently test the [redacted]." Internal Audit concluded that "[redacted]" testing, to include [redacted], was needed to provide the requisite "reasonable assurance" and sufficiency for remediation of the MRA. According to the Internal Audit memorandum, Internal Audit contemplated that [redacted] testing would include tests of [redacted] and would involve [redacted] within [redacted], [redacted], and verification of [redacted].

[4] The DER guidance prior to 2013-DER-OPB-01 and 2014-DER-OPB-02 did not require the issuance of a non-objection letter.

[5] The second remedial plan described the deliverables that had been completed and delivered to DER for three of the four initiatives in the initial remedial plan: (1) [redacted], (2) Enterprise [redacted] program, and (3) [redacted].

Freddie Mac management agreed to develop a third remedial plan that would include its commitment to perform [redacted] testing.

The third remedial plan represented that Freddie Mac would test [redacted]: "[redacted]." This plan stated that [redacted] testing would be performed for a "critical sampling of the [redacted] environment from both a [redacted] perspective." It also provided target dates for developing and executing a testing plan, and then validating and reporting on the testing results. The revised plan established an expected completion date of September 30, 2015. After review, DER issued a non-objection letter to this plan.

* * *

On September 27, 2017, we issued an audit report on our assessment of FHFA's efforts to complete planned supervisory activities related to cybersecurity risks at Freddie Mac for the 2016 examination cycle.[6] We found that for the 2016 examination cycle, DER completed four of the six cybersecurity-related supervisory activities it planned, one of which was an ongoing monitoring activity on Freddie Mac's efforts to remediate a cybersecurity-related MRA issued in 2012 relating to its ineffective and inadequate [redacted].

In this audit, we built upon that work. For the Freddie Mac MRA closed during the 2016 examination cycle relating to its ineffective and inadequate [redacted], we first sought to determine whether FHFA examiners followed existing requirements in issuing non-objection letters to Freddie Mac's remedial plans. We then assessed whether DER followed its guidance in independently verifying Freddie Mac's implementation of its remediation plans.

[6] OIG, *FHFA Did Not Complete All Planned Supervisory Activities Related to Cybersecurity Risks at Freddie Mac for the 2016 Examination Cycle* (Sept. 27, 2017) (AUD-2017-011) (online at www.fhfaoig.gov/Content/Files/AUD-2017-011%20FRE%20Cyber%20Examinations%20%28redacted%29.pdf).

FACTS AND ANALYSIS

While DER Issued Non-Objection Letters for Freddie Mac's Remedial Plans, None of These Plans Addressed a Critical Element in the MRA

This MRA issued from a 2011 information technology targeted examination of Freddie Mac and a 2011 targeted examination of Freddie Mac's [redacted] framework. In the targeted examination of Freddie Mac's [redacted] framework, DER found operational weaknesses in Freddie Mac's [redacted] for [redacted]. DER identified in the MRA the need for Freddie Mac to develop, as part of its [redacted] program, a process for "verifying and monitoring [redacted] programs and [redacted]."

Pursuant to DER Operating Procedures Bulletin (OPB) 2013-DER-OPB-1, *Matters Requiring Attention (MRA) Process* (April 23, 2013), which was in effect when Freddie Mac submitted its second and third remedial plans, those plans should have set forth, with sufficient detail, a process for "verifying and monitoring [redacted] programs and [redacted]." Our review of Freddie Mac's three remedial plans for this MRA, dated February 2012, August 2013, and November 2014, identified no planned steps to address [redacted] programs and [redacted] and we found no evidence in DER's system of records that DER brought the omissions in the remedial plans to Freddie Mac's attention and/or sought a supplemental plan to address this deficiency. We asked FHFA in December 2017, to "identify which remediation action plan key action addresses how Freddie Mac's management will 'provide for verifying and monitoring [redacted] programs and [redacted].'" FHFA responded on January 8, 2018, and confirmed the lack of a milestone to verify and monitor [redacted] programs and [redacted]:

> We have submitted to you our analysis memorandum that, to our knowledge, represents DER's complete assessment of Freddie Mac's remediation plans. We note that the written assessment does not directly address that Freddie Mac's [redacted] program should include verifying and monitoring [redacted] programs and [redacted]. However, in discussion with the Freddie Mac Operational Risk Exam Manager, [redacted] **is being proposed for the 2018 examination plan** (scheduled for approval by January 31, 2018).[7] (Emphasis added.)

[7] We note that DER's approved 2018 examination plan did not include [redacted] and planning capability as a specific examination objective.

Accordingly, we found that Freddie Mac's remedial plans failed to propose measures to address one of the critical deficiencies giving rise to this MRA.

DER Documents Reflect that DER Conducted an Independent Assessment in 2016 of Freddie Mac's Closure Package for the MRA

DER's Standard for Conducting its Assessment on Whether to Close an MRA: Was the Remedial Plan Fully Implemented as Intended

At the time DER was considering whether to close this MRA, three OPBs were in effect: 2013-DER-OPB-01; 2014-DER-OPB-01, *Guidelines for Preparing Supervisory Products and Examination Workpapers* (January 27, 2014); and 2014-DER-OPB-02, *Use of the Work of the Enterprise's Internal Auditor* (October 31, 2014).[8] As discussed earlier, 2013-DER-OPB-01 required DER examiners to review each proposed remedial plan to determine whether the identified corrective actions are "sufficiently detailed and appropriate" to resolve the deficiencies giving rise to the MRA. That OPB, 2014-DER-OPB-01, and 2014-DER-OPB-02, when read together, established the process to be used to assess whether an MRA should be closed:

- Determination by management upon completion of the remedial plan that the Enterprise has remediated the MRA,
- Review by the Enterprise's Internal Audit function or an independent third party to "'validate' that the action plan was implemented as intended and that the remediation is complete,"[9]
- Submission by the Enterprise of management's determination that the MRA has been remediated along with documentation of the independent validation work performed,
- Assessment by DER examiners of the Enterprise's remediation of the MRA. As needed, examiners would conduct necessary reviews to "validate" the remediation,

[8] DER-OPB-03.2, *Adverse Examination Findings Issuance and Follow-up* (June 21, 2017), rescinded and replaced 2013-DER-OPB-01 and 2014-DER-OPB-02. Among other things, the current OPB requires: examiners to review remedial plans to ensure proposed corrective action(s) is sufficient to address the MRA and, based on review of examiner work, the examiner-in-charge determines whether the MRA has been satisfactorily addressed.

[9] For further discussion of FHFA guidance and policies governing the respective roles of Enterprise Internal Audit and FHFA examination staff in assessing whether MRAs have been satisfactorily remediated, see *FHFA's Adoption of Clear Guidance on the Review of the Enterprises' Internal Audit Work When Assessing the Sufficiency of Remediation of Serious Deficiencies Would Assist FHFA Examiners* (Mar. 28, 2018) (EVL-2018-003) (online at www.fhfaoig.gov/reports/auditsandevaluations).

- Preparation of an analysis memorandum to document the results of the examiner's analysis of the Enterprise's closure package and Internal Audit's validation,
- Determination by the examiner as to whether the MRA has been addressed, and
- Communication of the determination to the Enterprise.

Because 2013-DER-OPB-01 and 2014-DER-OPB-02 directed DER to determine, when the remedial plan was first submitted, whether the identified corrective actions in it were "sufficiently detailed and appropriate" to resolve the deficiencies giving rise to the MRA, it stands to reason that the closure assessment required of DER in this OPB was tied to whether (1) "the action plan was implemented as intended" and (2) "the remediation is complete."

When, as here, the proposed remedial plan fell short of addressing all deficiencies giving rise to an MRA,[10] the OPB standard for closure assessment is too narrow, which DER acknowledged to us in its January 8, 2018 written response discussed above. In that written response, DER confirmed that its closure assessment did not evaluate whether Freddie Mac remediated a critical deficiency underlying the MRA: verifying and monitoring [redacted] programs and [redacted]. In technical comments to a draft of this report, FHFA asserted, for the first time, that Freddie Mac's third remedial plan, which included a key milestone to "produce memorandums of understanding (MOU) or equivalent with [redacted]," addressed the MRA deficiency relating to verification and monitoring [redacted] and [redacted].

Our review of this milestone in the third remedial plan and related documents found that the referenced MOUs were established as part of a Freddie Mac [redacted] exercise to test its [redacted] with [redacted] and focused on Freddie Mac's notice to these [redacted] that it would be testing Freddie Mac's [redacted] and its [redacted]. We found no reference in these MOUs to Freddie Mac's efforts to verify and monitor the [redacted] programs and [redacted] of its [redacted]. Verification and monitoring [redacted] programs and [redacted] of [redacted]

[10] As discussed earlier, none of the proposed remedial plans submitted by Freddie Mac contained remedial actions to address the identified deficiency of failing to verify and monitor [redacted] programs and [redacted]. In notes taken by a DER examiner of a Feb. 22, 2016, meeting between DER and Freddie Mac, we found reference to a statement by an Internal Audit representative that the [redacted] component of this MRA was viewed by Internal Audit as an integral component of the entire [redacted] program. However, those notes reflect that Internal Audit had not conducted validation testing of Freddie Mac's efforts to verify and monitor [redacted] programs and [redacted].

[redacted] is not the same as [redacted] testing by Freddie Mac to see if its [redacted] can [redacted] to its [redacted].

Accordingly, we cannot credit FHFA's claim because we found no evidence that this milestone in the third remedial plan addressed this MRA critical deficiency.

In August 2015, Freddie Mac Management Prepared its MRA Closure Package for Validation by Internal Audit

In August 2015, Freddie Mac management prepared a closure package for this MRA. Its then-Senior Vice President of Enterprise Operational Risk Management (the responsible management official for remediation of this MRA), attested in writing that:

- The root cause was adequately addressed by the actions taken.
- Remediation is complete.
- There is sufficient evidence to demonstrate remediation was implemented as intended.
- Operating effectiveness was adequately validated/demonstrated during the period and actions are sustainable.

This written attestation, along with supporting documents, was provided to Internal Audit to perform validation testing.

In October 2015, Freddie Mac's Internal Audit Concluded that the Remedial Plan Was Completed as Intended but Testing Was Not Sufficient to Provide Reasonable Assurance of the Adequacy of Freddie Mac's [redacted]

According to 2013-DER-OPB-01 and 2014-DER-OPB-02, the purpose of testing by Internal Audit was to validate whether (1) the remedial plan was implemented as intended and (2) remediation was complete. In a memorandum to Freddie Mac management dated October 16, 2015, Internal Audit concluded that "[m]anagement's action plan was completed as intended."

As discussed, Freddie Mac's third remedial plan required [redacted] testing for a "critical sampling of the [redacted] from both a [redacted] and [redacted] perspective" for three integrated business processes [redacted], with dates by which a testing plan would be developed and executed. This remedial plan did not provide further details on the scope or breadth of the [redacted] testing for this "critical sampling." Freddie Mac's Internal Audit was not satisfied with the breadth of the completed [redacted] testing and with the limitations on the scope of that testing. For those reasons, Internal Audit

advised management that "testing was not sufficient to provide reasonable assurance that Freddie Mac can effectively [redacted] due to limitations in the test scope, technology, and operations." Internal Audit declined to render an opinion on whether remediation was complete and cautioned, "we believe additional testing is required to provide reasonable assurance that [redacted] can be [redacted]."[11]

DER's Independent Assessment of the Closure Package

In a May 2016 Analysis Memorandum, DER documented its review of Freddie Mac management's closure package and the results of its ongoing monitoring of the progress of Freddie Mac's remediation of the MRA. It provided a written summary chronology of key events between 2012 and 2016 relating to the remediation of the MRA. That chronology included Freddie Mac's remedial plans, meetings DER held with Freddie Mac management and Internal Audit, Internal Audit's PIRs, and submission of Freddie Mac's closure package.

The Analysis Memorandum expressly identified the issues raised by Freddie Mac Internal Audit. It reported on a February 2016 meeting between DER and Freddie Mac management and Internal Audit that was called "to address an apparent discrepancy between [Freddie Mac] management and [Freddie Mac Internal Audit]." The Analysis Memorandum also reported that Internal Audit, in its October 16, 2015, memorandum on the validation testing for the closure package, identified serious concerns with regard to the sufficiency of [redacted] testing. According to the Analysis Memorandum, Internal Audit maintained that additional [redacted] testing was required in order to have reasonable assurance that the deficiencies underlying the MRA had been remediated. It further reported that Freddie Mac management recognized that [redacted] testing was an ongoing process that would not be completed for years.

The Analysis Memorandum reflected that DER reviewed Internal Audit's workpapers and other evidence submitted by Freddie Mac to demonstrate that the corrective action items and/or milestones in the August 30, 2013, and November 12, 2014, remedial plans were met. It stated that DER also reviewed [redacted], [redacted], [redacted] and [redacted] guidelines, test plans, test results, and a contractor's report on the testing results. This memorandum contained links to the documents reviewed by DER. While Freddie Mac Internal Audit concluded that the remedial plans were completed as intended, DER concluded in its Analysis Memorandum that "from our independent analysis and review of [Freddie Mac Internal Audit] evaluation that Freddie Mac

[11] According to Freddie Mac's Internal Audit policy then in effect, when Internal Audit reports on its follow-up of an MRA and concludes that Freddie Mac management implemented its action plan, the report is to state, "[m]anagement's action plan was implemented as intended *and remediation is complete*." (Emphasis added.) Internal Audit officials told us the omission of the language "remediation is complete" from Internal Audit's conclusion statement in the Oct. 16, 2015, memorandum was a conscious decision.

has satisfactorily remediated the MRA, with the exception of successful completion of [redacted] testing."

By letter dated May 18, 2016, DER notified Freddie Mac that it considered the MRA to be "satisfactorily addressed," based on its review of the remediation efforts and the validation testing by Internal Audit. It noted, however, that the remedial plan included [redacted] testing that was "not yet complete" and "Freddie Mac's [redacted] testing is expected to be continuous." DER stated that it intended to continue to monitor the effectiveness of the remediation, including Freddie Mac's testing of its [redacted] and [redacted] program, through future examination activity "as appropriate."

We sought to understand the basis on which DER closed the MRA in light of its determination that [redacted] testing was not yet complete. According to DER's Analysis Memorandum and the examiners who prepared that memorandum, the [redacted] testing for a "critical sampling of the [redacted] from both a [redacted] and [redacted] perspective" was, in fact, completed. (Freddie Mac Internal Audit reached the same conclusion.) That completed testing identified five issues for which follow-up was required, and those issues were being tracked by Internal Audit. Those follow-up issues, however, fell outside the milestones identified in the remedial plans and, under the OPB standard, would not have been relevant to DER's decision to close the MRA.

We also recognized the disparity between Internal Audit's admonition that the completed [redacted] testing was "not sufficient to provide reasonable assurance that Freddie Mac can effectively recover [redacted] timely due to limitations in the test scope, technology, and operations" and DER's conclusion that Freddie Mac had "satisfactorily remediated the MRA." In our view, that disparity was driven by DER's application of the OPB standard. Freddie Mac's third remedial plan proposed to conduct [redacted] testing for a "critical sampling" of the [redacted] for [redacted], but provided limited details about the scope or breadth of that sampling, and DER issued a non-objection letter to that plan.

Upon completion of the remediation, Internal Audit advised that it was not able to validate whether the deficiencies underlying the MRA had been addressed because of the limited testing. However, the OPB standard for validation testing and closure assessment is a different, and arguably narrower, standard: that standard is limited to whether implementation of the remedial plan was completed as intended. Because none of Freddie Mac's remedial plans identified the scope or breadth of the [redacted] testing, application of the OPB standard led DER to close the MRA.

We reviewed the work performed by the DER examiners, as documented in the Analysis Memorandum and supporting documents linked in that Analysis Memorandum. For all of these reasons, we found that DER satisfied the OPB standard when it closed this MRA.

That said, the deficiencies that gave rise to this MRA appeared to remain after the MRA was closed. We found that, in 2010, Internal Audit reported to Freddie Mac a management-identified issue with [redacted] that was substantially similar to those that gave rise to this MRA and tracked them as a uniquely identified major issue. Roughly seven years later (and eight months after DER closed this MRA), Internal Audit, in January 2017, closed out that major issue. The closure, however, was not because Internal Audit found that this major issue had been remediated. According to a memorandum prepared by Internal Audit, Freddie Mac management identified 13 new issues related to [redacted] (3 major issues and 10 other issues) during 2015 and 2016[12] and Internal Audit identified another major issue in a 2016 [redacted] internal audit. In short, Internal Audit concluded that the 13 issues identified by Freddie Mac management and the major issue it identified provided a more effective representation of the company's 2017 [redacted] risk profile, highlighted specific current limitations in the [redacted], and better defined accountability for ownership and remediation.

FINDING

DER Did Not Object to Freddie Mac's Remedial Plans Although those Plans Failed to Address All Critical Deficiencies Giving Rise to the MRA

FHFA's AB 2012-01 required each Enterprise to respond to an MRA with a proposed written remedial plan, including specific milestones taking into consideration the complexity of the issue and the urgency regarding correction. From 2012 to 2014, Freddie Mac submitted three remedial plans to DER for this MRA.

Pursuant to 2013-DER-OPB-01 and 2014-DER-OPB-02, DER examiners were tasked with reviewing two of the three proposed remedial plans to determine whether they were sufficiently detailed and appropriate to resolve the MRA. DER issued non-objection letters for two of the three plans. However, we found that none of the plans included steps to address a critical deficiency relating to verifying and monitoring [redacted]

[12] The three major issues identified by Freddie Mac management were: (1) [redacted] (identified Feb. 5, 2015); (2) [redacted] (identified May 20, 2015); and (3) a need to [redacted] (identified June 30, 2015). These major issues were identified by Freddie Mac management before DER closed the MRA on May 18, 2016.

programs and [redacted]. We found no evidence in DER's system of records that DER brought the omission to Freddie Mac's attention and/or sought a supplemental plan. As a result, DER had no assurance that Freddie Mac developed, as part of its [redacted] program, a process for "verifying and monitoring [redacted] programs and [redacted]," which was a critical deficiency underlying this MRA.

CONCLUSION

We performed this audit to assess, for the Freddie Mac MRA closed during the 2016 examination cycle relating to its ineffective and inadequate [redacted], whether FHFA examiners followed existing requirements in (1) issuing non-objection letters to Freddie Mac's remedial plans and (2) independently verifying Freddie Mac's implementation of its remediation plans. We found that Freddie Mac submitted three remedial plans for this MRA, and DER did not object to any of the plans, even though when taken together or separately, none addressed all deficiencies underlying the MRA, in contravention of DER guidance in 2013-DER-OPB-01 and 2014-DER-OPB-02. Specifically, none of the plans submitted for this MRA included any steps to address [redacted] programs and [redacted].

We also found that DER followed its standard in closing the MRA in that it independently verified that the actions in the proposed remedial plans, to which it issued non-objection letters, were implemented.

RECOMMENDATIONS

We recommend that FHFA:

1. Train DER examiners on the elements of the current OPB standard[13] for MRA issuance, follow-up and closure, which include: (a) a requirement that examiners ensure that proposed corrective actions in remedial plans are sufficient to address the deficiency underlying an MRA before issuing non-objection letters; and (b) a requirement that examiners determine, after an Enterprise implements its remedial plan, that the deficiency giving rise to the MRA has been satisfactorily addressed.

[13] DER-OPB-03.2, *Adverse Examination Findings Issuance and Follow-up* (June 21, 2017).

2. Ensure that Freddie Mac takes, or has taken, remedial action to address the deficiency underlying the MRA regarding the need to implement a process to verify and monitor the [redacted] programs and [redacted] of its [redacted].

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, which we incorporated as appropriate. In its management response, which is included in the Appendix to this report, FHFA agreed with our recommendations. In response to recommendation 1, FHFA stated that DER provided training on DER-OPB-03.2 to all DER examination staff in June 2017. According to FHFA, DER is currently working to revise and update DER-OPB-03.2. By December 31, 2018, DER will provide training to all examination staff (including examiners-in-charge and examination managers) on the provisions of the revised OPB with regard to the requirements that examiners should follow for MRA issuance, follow-up, and closure. In response to recommendation 2, FHFA stated that by March 22, 2019, DER will complete an examination activity that includes an assessment of Freddie Mac's process to verify and monitor the [redacted] and [redacted] of its [redacted]. We consider FHFA's planned corrective actions responsive to our recommendations.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of our audit was to assess, for the one Freddie Mac MRA closed during the 2016 examination cycle relating to its ineffective and inadequate [redacted], whether FHFA examiners followed existing requirements in (1) issuing non-objection letters to Freddie Mac's remedial plans and (2) independently verifying Freddie Mac's implementation of its remediation plans.

To address our objective, we:

- Researched and identified applicable laws and regulations related to Internal Audit verifying that MRAs are satisfactorily addressed.
- Researched and identified applicable guidance that relate to FHFA's documentation requirements and FHFA's process for verifying Freddie Mac's remediation of MRAs;
- Obtained and analyzed FHFA and/or Freddie Mac documentation and correspondence related to FHFA's verification of Freddie Mac's remediation of a cybersecurity MRA;

- Obtained and analyzed FHFA's Quality Control review results related to their review of FHFA's verification of Freddie Mac's remediation of a cybersecurity MRA;
- Interviewed FHFA officials to gain an understanding of its verification of Freddie Mac's remediation of a cybersecurity MRA; and
- Interviewed Freddie Mac's Internal Audit officials to gain an understanding of their verification of Freddie Mac management's remediation of a cybersecurity MRA.

We conducted this performance audit from September 2017 through March 2018 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 the 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 A. Freedman, Deputy Inspector General for Audits

FROM: Nina A. Nichols, Deputy Director, Division of Enterprise Regulation (DER) NAN

SUBJECT: Draft OIG Report: *FHFA Failed to Ensure Freddie Mac's Remedial Plans for a Cybersecurity MRA Addressed All Deficiencies; as Allowed by its Standard, FHFA Closed the MRA after Independently Determining the Enterprise Completed its Planned Remedial Actions*

DATE: March 22, 2018

This Memorandum transmits the management response of the Federal Housing Finance Agency (FHFA) to the FHFA Office of Inspector General's (OIG) draft report referenced above (Report).

We agree with the Report's conclusion that DER closed the specified Matter Requiring Attention (MRA) in accordance with examiner guidance, which included an assessment of whether the Enterprise remediation plan was implemented as intended and that the planned remediation was complete.

FHFA management's response to the recommendations are below.

Recommendation 1:

OIG recommends that FHFA train DER examiners on the elements of the current OPB standard[1] *for MRA issuance, follow-up and closure, which include: (a) a requirement that examiners ensure that proposed corrective actions in remedial plans are sufficient to address the deficiency underlying an MRA before issuing "non-objection" letters; and (b) a requirement that examiners determine, after an Enterprise implements its remedial plan, that the deficiency giving rise to the MRA has been satisfactorily addressed.*

Management Response to Recommendation 1:

FHFA agrees with this recommendation. DER provided training on DER-OPB-03.2, *Adverse Examination Findings Issuance and Follow-Up* (June 21, 2017), to all DER examination staff at the DER division meeting on June 22, 2017. DER is currently working to revise and update DER-OPB-03.2, and follow-up training would be beneficial. Accordingly, by December 31, 2018, DER will provide training to all examination staff (including Examiners-in-Charge and examination managers) on the provisions of the revised Operating Procedures Bulletin with regard to the requirements that examiners should follow for MRA issuance, follow-up, and closure.

Recommendation 2:

OIG recommends that FHFA ensure that Freddie Mac takes, or has taken, remedial action to address the deficiency underlying the MRA regarding the need to implement a process to verify and monitor the [redacted].

Management Response to Recommendation 2:

FHFA agrees with this recommendation. By March 22, 2019, DER will complete an examination activity that includes an assessment of Freddie Mac's process to verify and monitor the [redacted].

cc: John Major, Internal Controls and Audit Follow-up Manager
Larry Stauffer, Acting Chief Operating Officer

---

[1] DER-OPB-03.2, *Adverse Examination Findings Issuance and Follow-up* (June 21, 2017).

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