REDACTED

Federal Housing Finance Agency
Office of Inspector General

As Allowed by its Standard, FHFA Closed Three Fannie Mae Cybersecurity MRAs after Independently Determining the Enterprise Completed its Planned Remedial Actions

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

Audit Report • AUD-2018-007 • March 28, 2018

AUD-2018-007

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.

This audit is a follow-on to our audit report *FHFA Failed to Complete Non-MRA Supervisory Activities Related to Cybersecurity Risks at Fannie Mae Planned for the 2016 Examination Cycle* (AUD-2017-010) (September 27, 2017). In that audit, we assessed FHFA's efforts to complete planned supervisory activities related to cybersecurity risks at Fannie Mae for the 2016 examination cycle. For the 2016 examination cycle, DER planned, based on its 2016 supervisory plan as revised mid-year, to conduct one targeted examination at Fannie Mae, three ongoing monitoring activities relating to cybersecurity risks at Fannie Mae, and ongoing monitoring activities regarding Fannie Mae's efforts to remediate three cybersecurity-related Matters Requiring Attention (MRAs). We determined from that audit that, other than the ongoing monitoring activities to close the MRAs, DER did not complete any of its supervisory activities (the targeted examination and three ongoing monitoring activities) relating to Fannie Mae's cybersecurity risks planned for the 2016 examination cycle. We are building upon our previous audit work to determine, for the three cybersecurity MRAs closed in 2016, whether FHFA examiners followed existing requirements in independently verifying Fannie Mae's implementation of its remediation plans.

DER's guidance when these MRAs were closed directed examiners to assess whether the Enterprise's remedial plans were implemented as intended and that the planned remediation for each MRA was complete. For all three MRAs, we found that DER independently verified Fannie Mae's implementation of its remedial plans and met its standard in closing these MRAs. That said, for the MRA related to "[redacted]," DER examiners documented that concerns about the state of Fannie Mae's [redacted] remained and that DER intended to [redacted].

We make no recommendations in this report.

We are also issuing today the results of our audit of FHFA's verification of Freddie Mac's remediation of a cybersecurity related MRA. See *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*

AUD-2018-007

March 28, 2018

Actions (AUD-2018-008), online at www.fhfaoig.gov/reports/auditsandevaluations.

Key contributors to this report were: Jackie Dang, IT Audit Director; Dan Jensen, 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
[redacted]	[redacted]
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
OPB	Operating Procedures Bulletin

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.

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, (2) violations, and (3) recommendations.[1]

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." FHFA requires 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.

Once Fannie Mae determines that the remedial plan has been fully implemented and all planned remediation is complete, it submits a final deliverable memorandum outlining any completed remedial activities not previously communicated to DER, including evidence to support the completion of those activities. Also submitted to DER is evidence of validation testing conducted by Fannie Mae's internal audit function to determine whether the plan has been implemented and remediation is complete.[2]

---

[1] 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).

[2] See FHFA, 2013-DER-OPB-01, *Matters Requiring Attention (MRA) Process* (Apr. 23, 2013); Appendix to 12 C.F.R. § 1236 (Standard 2).

In this audit, we assessed whether DER followed its standard when it decided, during the 2016 examination cycle, that three cybersecurity-related MRAs issued in prior years were "satisfactorily addressed" and closed them. Specifically, we assessed whether DER followed its guidance by independently verifying Fannie's Mae implementation of its remedial plans.

We first provide background information on each of the three MRAs.

MRA Related to "[redacted]"

DER conducted a targeted examination in 2011 relating to Fannie Mae's management of information technology risks. In its Conclusion Letter dated February 24, 2012, DER reported on the results of this examination: Fannie Mae had not conducted a [redacted], including [redacted], since 2008 and issued an MRA for [redacted].

While DER acknowledged in the letter that Fannie Mae had successfully conducted [redacted] to the [redacted], it found that such [redacted]. DER cautioned that an actual [redacted] would likely [redacted]. DER further reported that a [redacted] test had been delayed until Fannie Mae completed a [redacted] Project).[3] It observed that the [redacted] Project had been postponed and "recently resurrected" with a projected completion date of September 2012. DER counseled that "Management should not postpone [the [redacted] Project] again and should accelerate its efforts to [redacted] capabilities and conduct [redacted]." DER projected that Fannie Mae's project to develop [redacted] capabilities would take "many more months."

Fannie Mae's Remediation Plan and DER's Non-Objection to that Plan

Fannie Mae submitted an initial remediation action plan for this MRA on March 23, 2012. That plan proposed: (1) completion of the [redacted] Project by September 30, 2012; (2) completion of [redacted] by December 31, 2012; (3) delivery of new [redacted] by September 30, 2013; and (4) [redacted] by September 30, 2014. At the time, FHFA did not require issuance of a "non-objection" letter and none was issued.

[3] According to DER, the [redacted] Project, and establishment of [redacted] (which were not part of that project), would facilitate more robust [redacted].

More than a year later, in September 2013, Fannie Mae submitted a revised remedial plan. The revised plan reported that the first two elements of the initial plan – the [redacted] Project and [redacted] – were completed. It changed the action item from delivery of [redacted] new [redacted] to [redacted] and delayed the targeted completion date to March 31, 2014. It also added a new action item: delivery of a project plan for an operationally ready, [redacted] and a testing strategy to ensure [redacted] with a targeted completion date of October 31, 2013. In light of these changes, it revised the fourth action item: complete [redacted] to the [redacted] by the planned completion date of September 30, 2014. DER issued a non-objection letter for this revised plan on December 20, 2013.

MRA Related to "[redacted]"

In July 2013, DER completed a targeted examination of Fannie Mae's controls around [redacted]. In its Conclusion Letter dated July 18, 2013, DER reported that its examination found significant risks and uncertainties in Fannie Mae's [redacted] and that these deficiencies warranted issuance of an MRA. While DER acknowledged that Fannie Mae had established [redacted] and remediation had taken place over a number of years to address these deficiencies, DER directed Fannie Mae to provide DER with a timetable to remediate these deficiencies, which prioritized the remedial actions and demonstrated that sufficient resources were dedicated to this remediation.

Fannie Mae's Remediation Plan and DER's Non-Objection to that Plan

Fannie Mae submitted a remediation action plan for this MRA on September 16, 2013. With respect to the deficiency for its [redacted], Fannie Mae proposed to implement a sustainable program to [redacted]. The targeted completion date to implement the program was December 15, 2013. It reported that its multi-year [redacted] program was underway and would demonstrate, by the end of the first year, complete "remediation tied to the [redacted] goal ([redacted] of the [redacted] included in the program) and funding year 2." DER issued a non-objection letter for this plan on October 7, 2013.

In an OIG evaluation issued in March 2016, we observed that Fannie Mae's remediation plan for the [redacted] failed to identify the specific deficiencies to be corrected and lacked any plan or milestones to remediate all of the shortcomings, contrary to DER requirements then in place. While its action item proposed to adopt a sustainable program to

[redacted] all [redacted] by December 15, 2013, and proposed to complete implementation of its plan for a portion of that [redacted] by year 1, we found that its plan did not identify the specific year 1 shortcomings that would be addressed and did not set forth a timeline to remediate the remaining unidentified shortcomings. Even though the Enterprise's remediation plan fell short, DER issued a non-objection letter to this plan on October 7, 2013. We also found that DER did not subsequently require the plan to be amended to identify the specific [redacted] to be remediated or to provide a timeline to complete remediation of the remaining unidentified unsupported software.[4] The plan remained unchanged until the MRA was closed by DER on December 27, 2016.

With respect to the deficiency of [redacted] in [redacted], Fannie Mae reported that, in the short term, it remediated this shortcoming by [redacted] (among other things). To remediate this deficiency in the long term, Fannie Mae reported that a completed [redacted] identified and mitigated potential [redacted] with respect to all [redacted]. Two remaining action items were identified, both with targeted completion dates of January 31, 2014:

- Develop an implementation plan to adopt the recommendations generated from the security assessment.
- Develop a plan to integrate the [redacted] into the [redacted] that would allow [redacted] concerns to be identified and addressed prior to [redacted].

DER issued a non-objection letter to this plan on October 7, 2013.

MRA Related to "[redacted]"

Another MRA issued from the same July 2013 targeted examination and was reported in the same July 18, 2013 Conclusion Letter. This MRA directed Fannie Mae to consolidate [redacted] into a [redacted] and to identify, in this system, both resolved and outstanding [redacted]. It instructed Fannie Mae to clearly define [redacted] for [redacted] resulting from [redacted]

[4] For a complete discussion of DER's approval of this remediation plan, see *FHFA's Examiners Did Not Meet Requirements and Guidance for Oversight of an Enterprise's Remediation of Serious Deficiencies* (Mar. 29, 2016) (EVL-2016-004) (online at www.fhfaoig.gov/Content/Files/EVL-2016-004.pdf).

[redacted], until resolved. DER directed that [redacted] should clearly define the [redacted] and role. Further, DER instructed that the Enterprise's [redacted] should clearly define [redacted] including the [redacted]. Last, it required Fannie Mae to make its [redacted] aware of the [redacted].

Fannie Mae's Remediation Plan and DER's Non-Objection to that Plan

By letter dated September 16, 2013, Fannie Mae informed DER that it had taken several actions to address the deficiencies underlying this MRA: (1) continued work by the [redacted] to optimize [redacted]; and (2) issued a revised [redacted] that outlined [redacted] for the [redacted] and [redacted], and included updated [redacted]. The letter committed to provide a remedial plan by November 15, 2013. That remedial plan, provided by the promised date, identified five action items with interim targeted completion dates, and a final targeted completion date of May 15, 2014. The five action items were: (1) enhance [redacted] with current [redacted] data – test [redacted] for then existing [redacted]; (2) [redacted] apply a [redacted] for enhanced [redacted]; (3) expand [redacted] – expand [redacted] capability to accommodate [redacted] from additional [redacted], such as [redacted]; (4) develop [redacted] – implement [redacted] for the [redacted] from the additional sources; and (5) consolidate reporting – aggregate [redacted] from multiple sources into [redacted] for senior management.

DER issued a non-objection letter for this remedial plan on January 24, 2014.

* * *

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 Fannie Mae for the 2016 examination cycle. We found that, other than the ongoing monitoring activities to close the MRAs, DER did not complete any of its supervisory activities (the targeted examination and three ongoing monitoring activities) relating to Fannie Mae's cybersecurity risks planned for the 2016 examination cycle.

In this audit, we built upon that work. For the three Fannie Mae cybersecurity MRAs closed during the 2016 examination cycle, 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 Fannie Mae's implementation of its remediation plans.

FACTS AND ANALYSIS

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 the MRAs, three DER internal examiner guidance documents, called Operating Procedures Bulletins (OPB), were in effect: 2013-DER-OPB-01, *Matters Requiring Attention (MRA) Process* (April 23, 2013); 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).[5] 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";[6]
- 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.

[5] 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.

[6] 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).

We were told by a DER examination manager for Fannie Mae that, in practice, this step was not undertaken until Internal Audit completed its work;

- Preparation of an analysis memorandum to document the results of the examiner's analysis of the Enterprise's work performed and Internal Audit's validation, if required by the examiner-in-charge;
- 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 was complete."

Closure of MRA Related to "[redacted]" Met DER's Standard

On September 30, 2014, Fannie Mae management submitted its final deliverable for this MRA. Preceding the September 2014 final deliverable were interim deliverables, each addressing an action item identified in the remedial plan and corresponding to the targeted completion date.[7] In its final deliverable, Fannie Mae reported that the planned [redacted] was stood up in May 2014, and a first [redacted] of the [redacted] was completed in September 2014. It represented in that deliverable: (1) "[e]stablishing the [redacted] has expanded Fannie Mae's [redacted] beyond [redacted] to include the more robust option of [redacted]"; and (2) "[t]he [redacted] program supports [redacted] necessary for Fannie Mae's most [redacted]." With its final deliverable, Fannie Mae included its testing documentation and a "high level" plan for future [redacted].

Fannie Mae's Internal Audit Concluded that Fannie Mae's Planned Corrective Actions Had Been Implemented

In a workpaper dated September 30, 2014, and provided to DER, Fannie Mae Internal Audit concluded that management's corrective actions had been implemented as of September 30, 2014. Internal Audit committed in the workpaper to continue to monitor subsequent [redacted] and to assess the overall strategy associated with the [redacted] of a then-existing

[7] The targeted completion date for one interim action item was missed by Fannie Mae, but not by a significant length of time. The targeted completion date for the final action item was met.

[redacted], prior to October 15, 2015. Internal Audit provided its monthly tracking reports on the progress of the remediation for this MRA to DER. In a tracking report dated December 15, 2015, Internal Audit "verified" that the planned remedial actions for this MRA were completed.

DER Closed this MRA Based on its Independent Review of Fannie Mae's Remedial Actions

In December 2016, DER documented in an Analysis Memorandum management's remediation efforts and the work performed by Fannie Mae Internal Audit. Based on its assessment of that work, DER determined that the Enterprise completed the planned remedial actions within agreed-upon timeframes.[8] That memorandum included a chart that identified each "Remediation Action Plan Item," described the action taken, and provided links to Fannie Mae remediation-related and Fannie Mae Internal Audit documents. The Analysis Memorandum reported that management's remediation efforts and the work performed by Fannie Mae's Internal Audit to validate remediation of the MRA were reviewed and "[w]e consider this MRA to be satisfactorily addressed." The Analysis Memorandum also stated that DER continued to have [redacted] of Fannie Mae's [redacted], even though Fannie Mae had satisfactorily completed the steps outlined in its remedial plan. DER observed that "[redacted] including a fully tested [redacted] is [redacted] to Fannie Mae's [redacted] program that enables the Enterprise to [redacted] within its [redacted]." Based on these [redacted] the Analysis Memorandum represented that DER intended to [redacted]. Further, DER management told us that DR should be an ongoing concern of the Enterprise and, therefore, the subject of ongoing monitoring.[9]

We reviewed the Analysis Memorandum and supporting documents and found that DER examiners followed established DER guidance in that they traced the planned remedial actions to the completed actions and independently reviewed supporting documentation. We found that the Analysis Memorandum linked to documents addressing each action item. For

[8] Although Fannie Mae notified DER during 2013 and 2014 as it completed action items in its remedial plan, DER's internal documents report that DER began its review of the MRA remediation after Internal Audit validated that the planned remedial actions were completed.

[9] In a Supervisory Letter dated Dec. 27, 2016, DER informed Fannie Mae that DER considered the MRA to be satisfactorily addressed "as Fannie Mae has satisfactorily completed the steps outlined in the remediation action plan submitted to DER for non-objection." The Supervisory Letter also reported the [redacted] of Fannie Mae's [redacted] and that DER [redacted]. DER's examination plans for both 2017 and 2018 included as planned supervisory activities ongoing monitoring of Fannie Mae's [redacted], including the Enterprise's development and implementation of an [redacted].

example, for the action item related to completion of the [redacted] Project, the Analysis Memorandum linked to documents such as one that showed [redacted] moved and [redacted] moved. For another action item related to the [redacted], there was a project plan for the build of the [redacted], a test plan for a [redacted] of the [redacted], and the results of [redacted] from that [redacted]. The Analysis Memorandum also provided links to Internal Audit's workpapers and supporting documents.

Closure of MRA Related to "[redacted]" Met DER's Standard

Prior OIG Evaluation Found that DER's Monitoring of MRA Remediation through October 2015 Did Not Meet DER's Guidance

As discussed earlier, our prior evaluation found that Fannie Mae's proposed remediation plan did not address all shortcomings in the MRA, but DER issued a non-objection to the plan. We also found shortfalls in DER's ongoing monitoring of Fannie Mae's efforts to remediate the [redacted] aspect of this MRA, which included:[10]

- Failure to Prepare a Procedures Document at the Outset of Monitoring. At the time DER issued the MRA in July 2013, DER's guidance then in effect directed DER examiners to prepare a Procedures Document identifying the intended examination steps to monitor an Enterprise's remediation of an MRA and to provide quarterly updates reporting on the supervisory activity during that period. We found that no timely Procedures Document was prepared, which DER acknowledged. Although the then-examiner-in-charge asserted that examiners prepared analysis memoranda to document their ongoing assessments of Fannie Mae's remediation, DER provided no such memoranda to us in response to our requests.

- Examiner Follow-up on Fannie Mae's Remediation Efforts Was Insufficient. We reported that DER examiners attended frequent meetings with Fannie Mae staff to discuss the progress of remedial efforts, review materials provided by Fannie Mae on its ongoing remediation, and track the progress of remediation. While we recognized that these examiners learned about the progress of MRA remediation from these meetings and documents, we found that existing FHFA and DER guidance for ongoing monitoring of MRA remediation required more than passive receipt of reports and information from the Enterprise.

[10] OIG, *FHFA's Examiners Did Not Meet Requirements and Guidance for Oversight of an Enterprise's Remediation of Serious Deficiencies* (Mar. 29, 2016) (EVL-2016-004) (online at www.fhfaoig.gov/Content/Files/EVL-2016-004.pdf)

- DER Documentation of its Ongoing Monitoring Contained No Assessment of the Adequacy or Timeliness of the Remedial Actions. At that time, FHFA and DER guidance required examiners to document their ongoing monitoring of remediation efforts. The voluminous materials provided by DER of its ongoing monitoring consisted of materials prepared by Fannie Mae. Because we found no observations, assessments, or conclusions by DER examiners on the adequacy or timeliness of the ongoing remediation in these materials, we concluded that they failed to meet established FHFA and DER guidance.

Fannie Mae's Internal Audit Concluded that Fannie Mae's Planned Corrective Actions Had Been Implemented

In April 2016, Internal Audit reported its validation testing. It found that [redacted] of [redacted] dependent on [redacted] had been [redacted] based on its [redacted]. Internal Audit also found "no exceptions" to the remedial actions to address [redacted]. Internal Audit concluded that Fannie Mae implemented a sustainable program to update or replace [redacted] and to address [redacted].

DER Closed this MRA Based on its Independent Review of Fannie Mae's Remedial Actions

During our audit, we found that DER completed a Procedures Document in 2016 for this MRA. Our review of that Procedures Document found that it identified examiner assessments of ongoing remediation and included links to supporting documents. In an October 2016 Analysis Memorandum, DER documented its review of Fannie Mae's interim and final deliverables. (It also summarized the results of its ongoing monitoring of the progress of Fannie Mae's remediation of the MRA; we previously catalogued the shortcomings of that ongoing monitoring in an evaluation issued in March 2016.) The Analysis Memorandum reviewed Internal Audit monthly status reports, examiner memoranda, meeting notes, report notes, and management's interim and final deliverables and contained links to the supporting documents. Notwithstanding the shortfalls observed with DER's ongoing monitoring of the MRA remediation through October 2015, we found that the examiners' independent analyses of Fannie Mae's remedial actions met DER's standard and provided the basis for closure of the MRA. Our review of the Procedures Document, Analysis Memorandum, and supporting documents found that DER examiners followed established DER guidance: they traced the planned remedial actions to the completed actions and independently reviewed supporting documentation before reaching their conclusion that the MRA had been satisfactorily addressed.

Closure of MRA Related to "[redacted]" Met DER's Standard

On May 15, 2014, Fannie Mae submitted its final deliverable for this MRA, meeting the proposed timetable. Preceding the May 2014 final deliverable was a series of interim deliverables, each addressing one of the five action items identified in the accepted remedial plan and submitted on the targeted completion date. Among the items included in the final deliverable were [redacted] showing [redacted] from multiple sources pulled into [redacted] for use by [redacted].

Fannie Mae's Internal Audit Concluded that Fannie Mae's Planned Corrective Actions Had Been Implemented

Fannie Mae's Internal Audit reported, on October 28, 2015, that "management's comprehensive [redacted] reporting to [redacted] were continuing to operate during 2015." While Internal Audit did not state an overall conclusion that all planned corrective action had been implemented, it reported that Internal Audit had validated implementation of the action items in the May 15, 2014, final deliverable.

DER Closed this MRA Based on its Independent Review of Fannie Mae's Remedial Actions

DER's April 2016 Summary Memorandum assessed the remediation undertaken by Fannie Mae's Office of the [redacted], interim and final deliverables, Internal Audit's status reports, meeting notes, Fannie Mae's monthly risk forum reports, board of directors meeting minutes, and Internal Audit validation work. The memorandum contained links to the documents reviewed by DER. Based on its independent analyses of Fannie Mae's remedial actions, DER concluded that Fannie Mae completed the actions required to satisfactorily address the MRA.[11]

The Summary Memorandum stated that DER examiners assessed Fannie Mae's final and interim deliverables to FHFA, along with attached [redacted] as evidence of completion. The Summary Memorandum also linked to FHFA's meeting notes and Fannie Mae Internal Audit's related workpaper documentation. Our review of documents in DER's system of records found that Fannie Mae's remedial actions and Fannie Mae Internal Audit's documentation supported the basis for the examiner's conclusion. We found that DER's independent analyses of Fannie Mae's

[11] In a Supervisory Letter dated Aug. 15, 2016, DER informed Fannie Mae that FHFA considered the MRA to be satisfactorily addressed.

and Fannie Mae Internal Audit's documentation met DER's standard and provided it with a reasonable basis for closing the MRA.

CONCLUSION

We performed this audit to assess, for the three Fannie Mae cybersecurity MRAs closed during the 2016 examination cycle, whether FHFA examiners followed requirements, in place at the time, of independently verifying Fannie Mae's implementation of its remedial plans.

We found that Fannie Mae submitted remedial plans for these MRAs, and DER did not object to any of the plans. We found that DER followed its standard in closing the MRAs in that it independently verified that the actions in the proposed remedial plans, to which it issued non-objection letters, were implemented.

We noted in DER's supervisory records that Fannie Mae management and DER examiners expressed concerns about remaining risk related to Fannie Mae's [redacted], the subject of one of the MRAs closed during 2016. Based on its [redacted], DER [redacted] of Fannie Mae's [redacted] and [redacted] as [redacted]. Given the criticality of [redacted] to Fannie Mae's business, we believe this is a prudent course of action.

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 incorporated as appropriate. In its management response, which is included in the Appendix to this report, FHFA acknowledged our report.

OBJECTIVE, SCOPE, AND METHODOLOGY

We examined three cybersecurity-related MRAs closed during 2016:

- MRA related to "[redacted]"
- MRA related to "[redacted]"

- MRA related to "[redacted]

For each MRA, we sought to assess whether FHFA examiners followed existing requirements in independently verifying Fannie Mae'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 related to FHFA's documentation requirements and FHFA's process for verifying Fannie Mae's remediation of MRAs;
- Obtained and analyzed FHFA and/or Fannie Mae documentation and correspondence related to FHFA's verification of Fannie Mae's remediation of cybersecurity MRAs; and
- Interviewed FHFA officials to gain an understanding of its verification of Fannie Mae's remediation of cybersecurity MRAs.

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: *As Allowed by its Standard, FHFA Closed Three Fannie Mae Cybersecurity MRAs after Independently Determining the Enterprise Completed its Planned Remedial Actions*

DATE: March 26, 2018

We are in receipt of the Federal Housing Finance Agency Office of Inspector General's (OIG) draft report referenced above. The audit assessed whether DER followed examiner guidance in independently verifying the Enterprise's implementation of its remediation plans for three Matters Requiring Attention (MRAs).

We agree with the Report's conclusion that DER closed the specified MRAs in accordance with examiner guidance, after assessing whether the Enterprise remediation plan was implemented as intended and that the planned remediation was complete. Please feel free to contact me with any questions.

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

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