REDACTED

Federal Housing Finance Agency
Office of Inspector General

FHFA Failed to Complete Non-MRA Supervisory Activities Related to Cybersecurity Risks at Fannie Mae Planned for the 2016 Examination Cycle

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

Audit Report • AUD-2017-010 • September 27, 2017

AUD-2017-010

September 27, 2017

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.

The Enterprises store, process, and transmit significant amounts of financial data and personally identifiable information in connection with their mission to support the secondary mortgage market. FHFA recognizes that cybersecurity is a significant risk for both Enterprises in light of the frequency and sophistication of attacks on information technology systems of financial institutions. In its 2015 Performance and Accountability Report (PAR), the Agency identified its priorities for 2016 and stated that: "A key objective of FHFA's supervisory work will continue to be the effective oversight of how each Enterprise manages cyber risks and addresses vulnerabilities." During the 2016 supervisory cycle, the Deputy Director, DER, underscored the importance of cybersecurity examinations for the supervision of financial institutions. In her March 2016 response to an OIG evaluation report, she wrote: "cybersecurity is a critical area for risk management by financial institutions and should continue to be a principal focus for federal financial regulators."

We performed this audit to address two objectives. First, we sought to determine whether the supervisory activities planned by DER relating to Fannie Mae's cybersecurity risks for the 2016 examination cycle addressed the cybersecurity risks highlighted in its risk assessment and supervisory strategy, applying the standard adopted by FHFA. We found that DER did not establish such a link in its supervisory planning documents to the risks it identified in its Operational Risk Assessment. We were not able to confirm whether all the risks identified in the Operational Risk Assessment could be tracked to planned cybersecurity supervisory activities. We also could not determine whether the planned supervisory activities addressed the risks DER considered the most critical because DER did not identify which risks were the most critical in either the Operational Risk Assessment or the Supervisory Strategy.

Second, we sought to determine whether such planned supervisory activities for the 2016 examination cycle were completed during that cycle in light of FHFA's representations in its 2015 PAR that "a key objective of FHFA's supervisory work" during 2016 would be oversight of how Fannie Mae managed its cyber risk and addressed vulnerabilities. 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 three other ongoing monitoring activities regarding Fannie Mae's efforts to remediate Matters Requiring Attention (MRAs) issued by DER in prior years. In an August 8, 2016, memorandum discussing the mid-year revisions to the 2016 supervisory plan, DER staff reported: "a number of staffing and structural changes in 2016…directly impacted execution of the 2016 examination plan," and reported that all ongoing monitoring activities and targeted examinations were "descoped due to the limited time available due to the focus on MRA closure."

DER officials told us that it tracks the workflow of supervisory activities through a tool called eClearance. When an official identified as an "approver" by DER in eClearance "approves" a document, that document is considered official. Based on our review of information in DER's eClearance system, corroborated by interviews with DER examination managers, we determined that DER did not complete any of its supervisory activities relating to Fannie Mae's cybersecurity risks planned for the 2016 examination cycle during that cycle. However, DER did complete ongoing monitoring of Fannie Mae's remediation of three cybersecurity-related MRAs issued in prior years and closed them during the 2016 cycle.

In an audit issued on September 30, 2016, we found that DER failed to conduct and complete more than half of its planned targeted examinations of Fannie Mae for the 2012 to 2015 examination cycles and completed no targeted examinations planned for the 2015 examination cycle before the 2015 ROE issued. We reported that the reason repeatedly provided by DER examiners and the then-current examiner-in-charge (EIC) for this failure was resource constraints, notwithstanding the consistent position of DER leadership and FHFA senior leadership that DER had an adequate complement of examiners and its staffing levels had not adversely affected its ability to meet its supervisory responsibilities. In that audit, we cautioned:

> For a federal financial regulator, responsible for supervising two Enterprises that together own or guarantee more than $5 trillion in mortgage assets and operate in conservatorship, to fail to complete a substantial number of planned targeted examinations, including failure to complete any of its 2015 planned targeted examinations for Fannie Mae within the 2015 supervisory cycle, is an unsound supervisory practice and strategy.

We cannot reconcile DER's inability to complete its four planned supervisory activities relating to Fannie Mae's cybersecurity during the 2016 examination cycle with representations by FHFA, in its 2015 PAR, and by the Deputy

Director, DER, that cybersecurity supervisory activities would be a key objective of FHFA's supervisory work during the 2016 supervisory cycle. A reasonable inference drawn from the August 8, 2016, staff memorandum is that DER staff holds the view that DER lacked a sufficient complement of examiners to adequately perform its supervisory responsibilities. The stated rationale in that memorandum for descoping all ongoing monitoring activities and targeted examinations was "the limited time available due to the focus on MRA closure." DER's failure to complete any of its planned supervisory activities relating to Fannie Mae's cybersecurity risks during 2016, a stated key objective of FHFA's supervision during 2016, provides additional cause for concern about the soundness of DER's supervisory practices and strategy.

At the conclusion of each annual supervisory cycle, DER summarizes and communicates the results of its supervisory activities in an annual report of examination (ROE) issued to each Enterprise. The purpose of the ROE is to clearly communicate to each Enterprise board the examination conclusions, findings, and supervisory concerns from FHFA's supervisory activities completed during the annual examination cycle to assist Enterprise directors in carrying out their oversight responsibilities.

Because DER completed no planned supervisory activities during 2016 relating to management of cybersecurity risk by Fannie Mae (other than closing MRAs issued in prior years), it had no findings to report in the section of the ROE titled "Information Security and Cyber-Security." Lacking supervisory information relating to management of information security risks to report in this ROE, DER summarized the conclusions reached by Fannie Mae's Internal Audit function and by a contractor retained by Fannie Mae to perform a cyber risk assessment. There is a significant risk that DER's inability to complete any of its supervisory activities relating to Fannie Mae's management of its cybersecurity risks and reliance on conclusions reached by Fannie Mae's Internal Audit and its contractor deprives Fannie Mae's board of directors with information necessary to execute the cyber risk management responsibilities delegated to it by FHFA.

We make three recommendations to FHFA to address the shortcomings identified in this audit. In a written management response, FHFA agreed that cybersecurity is a significant area for risk management by the Enterprises and is a critical component of FHFA's supervision of the Enterprises. FHFA represented that it is working to improve its supervision protocols and processes to more effectively identify cybersecurity risks and address them in DER's examination activities. While FHFA disagreed with various statements in the report, it agreed with one recommendation and partially agreed with the

AUD-2017-010

September 27, 2017

other two recommendations. Its planned corrective actions are responsive to all three of our recommendations.

We are also issuing today the results of our audit of DER's execution and completion of planned supervisory activities for the 2016 examination cycle to test the adequacy of Freddie Mac's risk management of its cybersecurity risks. See *FHFA Did Not Complete All Planned Supervisory Activities Related to Cybersecurity Risks at Freddie Mac for the 2016 Examination Cycle*, AUD-2017-011, available online at www.fhfaoig.gov/reports/auditsandevaluations.

Key contributors to this report were Jackie Dang, IT Audit Director; David Cho, IT Specialist; Dan Jensen, 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 FHFA, 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

DER	Division of Enterprise Regulation
EIC	Examiner-in-Charge
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	Office of Inspector General
OPB	Operating Procedures Bulletin
PAR	Performance and Accountability Report
ROE	Report of Examination

BACKGROUND

DER's Supervisory Process

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 Enterprises 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. Like other federal financial regulators, FHFA maintains that it uses a risk-based approach to carry out its supervisory activities.

In a number of recently issued reports, we explained in detail the different elements of DER's supervision program for the Enterprises.[1] These elements include:

- DER's written assessment of risks at the Enterprises, which serves as a platform for developing its annual supervisory strategy and supervisory plan;
- DER's annual supervisory strategy, which is intended to form a bridge between the significant risks and supervisory concerns identified in the risk assessment and the supervisory activities to be conducted. The supervisory strategy should include, among other things, the planned supervisory approach (extent of ongoing monitoring or targeted examination activity) and planned objectives that address the significant risks and the principal supervisory priorities for the year;
- DER's supervisory plan for each annual examination cycle, which sets forth the planned supervisory activities, prioritized based on the level of risk identified in DER's risk assessments. According to FHFA guidance, the supervisory plan should clearly link to the supervisory strategy;
- Supervisory activities, including ongoing monitoring and targeted examinations. According to FHFA, ongoing monitoring and targeted examinations serve complementary purposes. The purpose of ongoing monitoring is to analyze real-time information and to use those analyses to identify Enterprise practices and changes in an Enterprise's risk profile that may warrant increased supervisory attention. Ongoing monitoring is also used to determine the status of the Enterprise's compliance with

[1] Recently issued OIG reports addressing DER's supervisory process are summarized in OIG, *Safe and Sound Operation of the Enterprises Cannot Be Assumed Because of Significant Shortcomings in FHFA's Supervision Program for the Enterprises* (Dec. 15, 2016) (OIG-2017-003) (online at www.fhfaoig.gov/Content/Files/OIG-2017-003.pdf).

supervisory guidance, MRAs, and conservatorship directives. Targeted examinations enable examiners to conduct "a deep or comprehensive assessment" of the areas found to be of high importance or risk;[2]

- DER's communication of its findings from its supervisory activities, including its supervisory concerns, to each Enterprise;
- DER's follow-up on efforts by each Enterprise to correct identified deficiencies throughout the remediation period to ensure that remediation is timely and adequate; and
- DER's communication of its examination conclusions, findings, and composite/component examination ratings after the end of each annual examination cycle to each Enterprise board of directors in an annual ROE to assist Enterprise directors in executing their oversight responsibilities.

FHFA Recognizes that Effective Management of Cybersecurity Is Critical to the Safety and Soundness of the Enterprises

The Enterprises store, process, and transmit financial data and personally identifiable information in connection with their mission to support the secondary mortgage market. As events over the past few years have shown, other institutions holding similar types of data have sustained significant cyber attacks. The Enterprises consistently recognize in their annual securities filings that there is no assurance that the precautions put into place to protect their data will be invulnerable to penetration and that a successful cyber attack could lead to substantial financial losses.

FHFA has highlighted supervisory concerns over information technology issues at the Enterprises in its public reports to Congress in each of the past five years. In its PAR issued in November 2015, FHFA acknowledged that information security "is a significant risk" for both Enterprises in light of the frequency and sophistication of attacks on information technology systems of financial institutions. In the section titled, "Looking Ahead to FY 2016," the Agency stated that '[a] key objective of FHFA's supervisory work will continue to be the effective oversight of how each Enterprise manages cyber risks and addresses vulnerabilities." The following year FHFA again recognized, in its PAR issued in November 2016, that threats to information security and the frequency and sophistication of cyber

[2] MRAs are adverse examination findings that fall into one of the following categories: (1) critical supervisory matters (the highest priority) that pose substantial risk to the safety and soundness of the Enterprise and (2) deficiencies that are supervisory concerns, which FHFA believes could, if not corrected, escalate and potentially negatively affect the condition, financial performance, risk profile, operations, or reputation of the Enterprise.

attacks are an area of focus for all financial service regulators and represented that "FHFA continues to adjust its supervision activities to address these evolving risks."

During the 2016 examination cycle, the Deputy Director, DER, underscored the importance of cybersecurity supervision for financial regulators. In a March 2016 response to an OIG evaluation report, the Deputy Director deemed cybersecurity "a critical area for risk management by financial institutions" and stated that it "should continue to be a principal focus for federal financial regulators."

FHFA has delegated responsibility for oversight of general corporate matters to each Enterprise's board of directors, including oversight of the risk management program, which includes cyber risk. FHFA has supplemented its general governance standards with supervisory expectations for board oversight and monitoring of an Enterprise's cyber risk management program set forth in its Advisory Bulletin (AB) 2014-05, *Cyber Risk Management Guidance*, May 2014. FHFA has also directed that the board of each of its regulated entity is responsible for having policies in place to assure oversight of the Enterprise's risk management program and of "[t]he responsiveness of executive officers…addressing all supervisory concerns of FHFA in a timely and appropriate manner." [3]

[3] 12 C.F.R. § 1239.4(c)(1), (3).

FACTS AND ANALYSIS

DER Failed to Link the 2016 Planned Supervisory Activities Relating to Fannie Mae's Cybersecurity Risks to the Risks Identified in its Operational Risk Assessment, as Required by FHFA

Operational Risk Assessment for the 2016 Examination Cycle

DER's Operational Risk Assessment for the 2016 examination cycle identified a number of cybersecurity risks for Fannie Mae. Among other things, it observed:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Overall, DER assigned a risk rating of [redacted][4]

Supervisory Strategy for the 2016 Examination Cycle

FHFA directs, in its *Examination Manual*, that the annual supervisory strategy forms a bridge between the risk assessment, which identifies significant risks and supervisory concerns, and the supervisory activities to be conducted. To provide more granular guidance to its examiners on the supervisory planning process, DER promulgated Operating Procedures Bulletin (OPB) 2013-DER-OPB-03.1, *Supervisory Planning Process*, which directs that the annual supervisory strategy should include certain minimum information:

- Planned supervisory approach (extent of ongoing monitoring or targeted examination activity), and
- Planned objectives that address the significant risks and the principal supervisory priorities for the year.

DER's 2016 Supervisory Strategy stated that FHFA will focus, as it relates to cybersecurity at Fannie Mae, on four broad areas of operational risk: [redacted][5]

Although the *FHFA Examination Manual* (and 2013-DER-OPB-03.1) instruct that the annual supervisory strategy provide specifics as to how the strategy will be implemented in the coming year, DER's 2016 Supervisory Strategy for Fannie Mae contained no information on the planned supervisory approach to address these four high-level risks.

DER's Supervisory Activities for the 2016 Examination Cycle

DER's 2016 Fannie Mae Supervisory Plan, as updated on June 29, 2016, planned the following activities involving cybersecurity:

[4] The *FHFA Examination Manual* identifies the risk ratings to be used in risk assessments and [redacted] is not included in its identified ratings. [redacted]

[5] Because these four key risks were far more general than what was presented in the Operational Risk Assessment, we asked the Examiner-in-Charge (EIC) to explain how these four key cyber risks were identified. He explained that the annual Supervisory Strategy was very broad and was not meant to get into the same level of detail as the Operational Risk Assessment. He reported that the assessment of risk in the Operational Risk Assessment drove the planned supervisory activities in the annual Supervisory Plan.

- One targeted examination,
- Three ongoing monitoring activities, and
- Three other ongoing monitoring activities regarding Fannie Mae's efforts to remediate MRAs issued by DER in prior years.

We sought to determine whether DER's planned supervisory activities addressed the cybersecurity risks identified by DER in its Operational Risk Assessment, using the standard in the *FHFA Examination Manual* and the guidance in 2013-DER-OPB-03.1. Our comparison of the cybersecurity risks identified in DER's Operational Risk Assessment for Fannie Mae to its Supervisory Strategy for 2016 and the stated objectives of the planned supervisory activities for 2016 found that DER did not establish a link between the objectives of the planned supervisory activities and the risks in the Operational Risk Assessment. We were not able to determine whether all the risks identified in the Operational Risk Assessment could be tracked to planned cybersecurity activities. For example, we identified two risks [redacted] – that were not included in the objectives for the planned supervisory activities.[6] We also could not determine whether the planned supervisory activities addressed the risks DER considered the most critical because DER did not identify which cyber risks were the most critical in the Operational Risk Assessment.

In its technical comments, FHFA sought to dismiss our inability to align the cybersecurity risks identified in DER's risk assessments with its planned supervisory activities on the grounds that "DER holds mid-year and year-end planning meetings, discussions of risk by risk area, and review and vetting of proposed changes to the examination plan for each Enterprise. Cybersecurity was discussed as part of the examination plan and risk assessment for operational risk during the 2016 planning meetings." Neither the *FHFA Examination Manual* nor the implementing guidance in 2013-DER-OPB-03.1 contemplate that undocumented discussions are an acceptable substitute for the certain minimum information required to be included in the annual supervisory strategy and objectives for the planned supervisory activities.

[6] FHFA asserted, in its technical comments, that a sub-objective of the "IT: Information Technology" ongoing monitoring activity addressed both of these risks. In light of those comments, we re-examined the Procedures *Document* for this ongoing monitoring activity and found that it did not support FHFA's assertion.

DER Failed to Complete Any of its Planned Supervisory Activities Related to Cybersecurity Risks at Fannie Mae during the 2016 Examination Cycle, Save for Three Ongoing Monitoring Activities to Oversee Fannie Mae's Remediation of MRAs Issued in Prior Years

Because FHFA announced in its 2015 PAR that "effective oversight of how each Enterprise manages cyber risks and addresses vulnerabilities" would be a "key objective of FHFA's supervisory work" during 2016, we examined whether DER examiners completed planned supervisory activities relating to Fannie Mae's cybersecurity risks during 2016.

DER's 2016 Fannie Mae Supervisory Plan, as updated on June 29, 2016, consisted of one targeted examination and three ongoing monitoring activities involving cybersecurity and three other ongoing monitoring activities regarding Fannie Mae's efforts to remediate MRAs issued by DER in prior years. Because supervisory planning is a continuous process, supervisory plans need to be adjusted during each year to address newly emerging risks that require attention during the current supervisory cycle. Beginning with the 2014 supervisory cycle, DER's guidance in 2013-DER-OPB-03.1 directs that approved supervisory plans shall only be adjusted for risk-related reasons, and justifications for the adjustments must be approved by the EIC (after consultation with the Deputy Director, DER, as warranted) and fully documented in the workpapers.

DER made a number of mid-year revisions to its 2016 supervisory plan. According to an August 8, 2016, memorandum prepared by DER staff to explain these mid-year revisions, "a number of staffing and structural changes in 2016…directly impacted execution of the 2016 examination plan." The memorandum explained that "approximately half of the [DER] staff is FHFA tenured with a year or less with the organization." It also reported that DER's focus during 2016 was on closing MRAs rather than responding to evolving risks.[7] Notwithstanding FHFA's representation in its 2015 PAR that a "key objective of FHFA's supervisory work" in 2016 "will continue to be the effective oversight of how each Enterprise manages cyber risks and addresses vulnerabilities," this memorandum reported that all operational risk (which includes information technology) planned ongoing monitoring activities and targeted examinations were "descoped due to the limited time available due to the focus on MRA

[7] In 2016, OIG published two reports highlighting issues with DER's closures of MRAs. *See* OIG, *FHFA's Inconsistent Practices in Assessing Enterprise Remediation of Serious Deficiencies and Weaknesses in its Tracking Systems Limit the Effectiveness of FHFA's Supervision of the Enterprises* (July 14, 2016) (EVL-2016-007) (online at www.fhfaoig.gov/Content/Files/EVL-2016-007.pdf); and 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). The cited March report highlighted an MRA that remained open and unresolved more than 30 months after issuance.

closure."[8] As a result of the mid-year revisions to the supervisory plan, one targeted examination was descoped, another was converted to an ongoing monitoring activity, and the other two ongoing monitoring activities were also descoped.

DER officials reported to us that DER tracks the workflow of supervisory activities through a tool called eClearance. When an official identified as an "approver" by DER in eClearance "approves" a document, that document is considered official. A DER official explained that a supervisory activity is considered completed once the supervisor signs off on the examination documentation. Applying this criteria, we found that the eClearance entries show that the approving official signed off on two ongoing monitoring activities relating to Fannie Mae's cybersecurity risks in May 2017 and on the third in June 2017, well after the 2016 supervisory cycle ended and the ROE for that cycle issued. As of September 2017, the targeted examination had not been completed (it was brought forward to the 2017 supervisory plan). DER completed three ongoing monitoring activities related to Fannie Mae's remediation of MRAs.[9]

We cannot reconcile DER's inability to complete its four planned supervisory activities relating to Fannie Mae's cybersecurity during the 2016 examination cycle with representations by FHFA in its 2015 PAR and by the Deputy Director, DER, that cybersecurity supervisory activities would be a key objective of FHFA's supervisory work during the 2016 supervisory cycle.

In its technical comments, FHFA argued that it is "inaccurate to suggest that DER performed no supervisory work relating to cybersecurity in 2016" because one of the three ongoing monitoring activities relating to Fannie Mae's cybersecurity management was completed in 2016 and reviewed by DER management in January 2017. In reviewing the eClearance workflow for this ongoing monitoring activity, we found that activity was not completed until May 23, 2017, when the EIC approved the completion memorandum. As we have explained, the scope of this audit did not include whether DER *performed* any supervisory work relating

[8] All three of the ongoing monitoring remediation activities planned to assess remediation of MRAs issued in prior examination cycles were completed [redacted] The ROE reported [redacted] open MRAs as of December 31, 2016, [redacted]

[9] FHFA stated in its technical comments that we "appear[ed] to dismiss the examination work performed to review the Enterprise's remediation work to address MRAs. Ongoing monitoring performed for this purpose is listed on annual examination plans as a separate activity for each MRA, given the importance of MRAs in identifying Enterprise risks." That comment ignores the observation we made multiple times throughout this audit report that DER completed three ongoing monitoring activities during the 2016 examination cycle related to Fannie Mae's remediation of MRAs issued in past years.

to cybersecurity in 2016. It assessed whether the supervisory activities relating to cybersecurity planned for the 2016 supervisory cycle were *completed* during that cycle.[10]

In an audit issued last year, we found that DER completed less than half of its 2012 through 2015 planned targeted examinations for Fannie Mae and did not complete many of its planned targeted examinations for each supervisory cycle prior to the issuance of the respective cycle's ROE to Fannie Mae.[11] For the 2015 supervisory cycle, we found that DER completed none of its 11 planned targeted examinations for Fannie Mae within that cycle. We reported that the reason repeatedly provided by DER examiners and the then-current EIC for this failure was resource constraints, notwithstanding the consistent position of DER leadership and FHFA senior leadership that DER had an adequate complement of examiners and its staffing levels had not adversely affected its ability to meet its supervisory responsibilities. In that audit, we cautioned:

> For a federal financial regulator, responsible for supervising two Enterprises that together own or guarantee more than $5 trillion in mortgage assets and operate in conservatorship, to fail to complete a substantial number of planned targeted examinations, including failure to complete any of its 2015 planned targeted examinations for Fannie Mae within the 2015 supervisory cycle, is an unsound supervisory practice and strategy.

We recommended that DER assess whether it had a "sufficient complement of qualified examiners to conduct and complete those examinations rated by DER to be of high-priority within each supervisory cycle and address the resource constraints that have adversely affected DER's ability to carry out its risk-based supervisory plans."

In its response dated September 22, 2016, DER did "not agree that current staffing levels have adversely affected DER's ability to meet its supervisory responsibilities."[12] Six weeks prior to

---

[10] FHFA also maintains in its technical comments that significant DER resources were dedicated in 2016 to developing an examination manual module on information security, which has not yet been finalized. We note that the August 8, 2016, memorandum only identified "the limited time available due to the focus on MRA closure" as the reason that targeted examinations and ongoing monitoring activities had been descoped. The EIC for the Fannie Mae examination team reported to us in July 2017 that DER made MRA remediation a high priority when compared to other supervisory work during the 2016 supervisory cycle. Neither the EIC nor any of the DER examination managers with whom we spoke suggested that planned supervisory activities relating to Fannie Mae's cybersecurity risks were not completed during 2016 because those examiner resources were dedicated to creating a new examination module.

[11] *See* OIG, *FHFA's Targeted Examinations of Fannie Mae: Less than Half of the Targeted Examinations Planned for 2012 through 2015 Were Completed and No Examinations Planned for 2015 Were Completed Before the Report of Examination Issued* (Sept. 30, 2016) (AUD-2016-006) (online at www.fhfaoig.gov/Content/Files/AUD-2016-006.pdf).

[12] FHFA did agree in its response that it was "a sound practice to regularly assess whether staffing levels are sufficient to carry out DER responsibilities for fulfillment of FHFA's mission."

issuing that response, DER staff issued the August 8, 2016, memorandum, discussed above, reporting that all planned ongoing monitoring activities and targeted examinations were "descoped due to the limited time available due to the focus on MRA closure." DER's workflow tool, eClearance, showed that none of the supervisory activities relating to Fannie's Mae's cybersecurity risks were completed during the 2016 supervisory cycle. A reasonable inference drawn from the August 8, 2016, staff memorandum is that DER staff holds the view that DER lacks a sufficient complement of examiners to adequately perform its supervisory responsibilities. DER's failure to complete any of its planned supervisory activities relating to Fannie Mae's cybersecurity risks during 2016, a stated key objective of FHFA's supervision during 2016, provides additional cause for concern about the soundness of DER's supervisory practices and strategy.

Although DER Failed to Complete Any Planned Supervisory Activities During 2016 Relating to Fannie Mae's Management of Cybersecurity Risks (Other than the Three Ongoing Monitoring Activities Relating to Remediation of Existing MRAs), the ROE for the 2016 Examination Cycle Reported Conclusions by DER on This Issue

According to FHFA, the ROE communicates to the board of directors: substantive examination conclusions, findings (when applicable), and the composite and component ratings. As the FHFA Director testified recently before the House Financial Services Committee, the ROE "capture[s] **FHFA's view** of the safety and soundness of each Enterprise's operations" (emphasis added).

Communication of supervisory concerns to Fannie Mae's board is critical. FHFA's governance regulations and the *FHFA Examination Manual* make clear that the board of a regulated entity is ultimately responsible for: ensuring that the conditions and practices that gave rise to any supervisory concerns are corrected and that executive officers have been responsive in addressing all of FHFA's supervisory concerns in a timely and appropriate manner, and holding management accountable for remediating those conditions and practices.[13] Only when an Enterprise board is presented by FHFA with sufficient information

[13] In two evaluation reports – issued before the 2016 ROE in question – we found that FHFA's limited ROE requirements and guidance and DER's shortcomings in following those standards weakened the value of the ROE to Enterprise boards and thus created the risk that Enterprise boards may not be fully knowledgeable of matters addressed in the ROE; as well, it constrained the boards' ability to oversee remediation of supervisory concerns. We found that FHFA had little assurance that the ROE would focus the attention of an Enterprise board on excessive risks or deficient risk management practices and their root causes, consistent with the objectives of FHFA's supervisory activities. *See* OIG, *FHFA's Failure to Consistently Identify Specific Deficiencies and Their Root Causes in Its Reports of Examination Constrains the Ability of the Enterprise Boards to Exercise Effective Oversight of Management's Remediation of Supervisory Concerns* (July 14, 2016) (EVL-2016-008) (online at www.fhfaoig.gov/Content/Files/EVL-2016-008.pdf); and OIG, *FHFA Failed to Consistently Deliver Timely Reports of Examination to the Enterprise Boards and Obtain Written Responses from the Boards Regarding Remediation of Supervisory Concerns Identified in those Reports* (July 14, 2016) (EVL-2016-009) (online at www.fhfaoig.gov/Content/Files/EVL-2016-009.pdf).

about the substantive examination results and conclusions, findings, and supervisory concerns can it effectively oversee management's efforts to correct deficiencies.

Save for the three ongoing monitoring activities to monitor Fannie Mae's efforts to remediate MRAs issued in prior years, we found that DER completed none of its planned cybersecurity supervisory activities before the 2016 ROE issued on March 3, 2017.[14] Because DER completed none of these activities during 2016, it reached no findings on any cybersecurity issues and was not in a position to issue (and did not issue) any findings related to its 2016 examination work on cybersecurity to report in the section of the ROE titled "Information Security and Cyber-Security."

Instead, DER discussed assessments provided from two Fannie Mae-related sources – by Fannie Mae's Internal Audit and by a consultant retained by Fannie Mae. The ROE reported that Fannie Mae's Internal Audit determined, in January 2016, that, among other things, [redacted] However, in the 15 months after the determinations by Fannie Mae's Internal Audit, DER completed no supervisory activities in any of those areas and, as a result, had no findings or supervisory concerns to report in the ROE. The ROE is silent on what progress, if any, was made by Fannie Mae during the 15 months between the determinations by Internal Audit, in January 2016, and the issuance of the ROE in March 2017.

Likewise, this section of the ROE reports that Fannie Mae retained an "independent cyber assessment" from a consultant. The ROE relayed that the consultant's report noted that Fannie Mae should [redacted] Other than reporting the views of the consultant retained by Fannie Mae, FHFA, as the supervisor of Fannie Mae, offered no supervisory perspective on those issues based on any completed examination work.

Only one sentence in the information security section of the ROE contains an apparent conclusion by DER: "[t]he Enterprise continues to develop its information security risk management program but [redacted] DER's conclusion—that [redacted]—was not tethered to examination work completed during the 2016 cycle. In its technical comments, FHFA did not take issue with this finding.

[14] The cybersecurity targeted examination, which was planned to be completed in September 2016, was not finished as of September 2017. Two ongoing monitoring activities were completed without findings in May 2017, and the third ongoing monitoring activity was completed in June 2017.

In 2015, we evaluated DER's efforts to establish an independent quality assurance review program.[15] We recommended that FHFA "[e]nsure that DER's recently adopted procedures for quality control reviews meet" FHFA's requirements and "require DER to document in detail the results and findings of each quality control review in examination workpapers, including any shortcomings found during the quality control review." In its written response, FHFA stated that it "agrees with this recommendation," and acknowledged that "a process for independent quality control of examination documentation is important to the supervision of Fannie Mae and Freddie Mac." The formal written guidance issued by DER in June 2016, Operating Procedures Bulletin DER-OPB-02, *Quality Control Review*, did not meet FHFA's requirements because it did not require quality control reviews of ROEs. We have previously reported that a senior DER official represented to us that no quality assurance review is required for ROEs because the underlying work reported in each ROE has been subject to such review.[16] Plainly, no quality assurance review was conducted for this conclusion as DER did not complete its supervisory activities on cybersecurity during 2016, in derogation of DER's own requirements in DER-OPB-02.

In another section of the 2016 ROE, titled [redacted] DER reported that Fannie Mae [redacted] We found no evidence that DER communicated any [redacted] during the 2016 examination cycle. [redacted] Again, we found no evidence that DER previously communicated this observation in writing to Fannie Mae, as required by DER-OPB-02. Because DER completed no supervisory activities relating to cybersecurity during 2016 and its statement and observation in this section of the ROE were not tied to other specific supervisory activities, we were not able to determine the support for this statement and observation as well as whether either had been subject to DER's quality control process.

In its technical comments, FHFA took issue with this finding and claimed that DER provided that observation, in writing, to Fannie Mae, in a letter dated December 27, 2016. We reviewed that letter, which notified Fannie Mae that DER closed a [redacted] DER stated, in that letter:

---

[15] *See* OIG, *Intermittent Efforts Over Almost Four Years to Develop a Quality Control Review Process Deprived FHFA of Assurance of the Adequacy and Quality of Enterprise Examinations* (Sept. 30, 2015) (EVL-2015-007) (online at www.fhfaoig.gov/Content/Files/EVL-2015-007.pdf).

[16] *See* OIG, *The Gap in FHFA's Quality Control Review Program Increases the Risk of Inaccurate Conclusions in its Reports of Examination of Fannie Mae and Freddie Mac* (Aug. 17, 2017) (EVL-2017-006) (online at www.fhfaoig.gov/Content/Files/EVL-2017-006.pdf)

> Fannie Mae has implemented operational changes since issuance of this MRA, and examination work conducted since issuance and remediation has identified risks associated with the overall state of [redacted] Accordingly, DER will conduct further supervisory work, which could potentially result in additional findings.

Plainly, DER's reference to "risks" identified since 2012 "associated with the overall state of Fannie's Mae's [redacted] did not provide Fannie Mae with written notice of a recommendation by DER that it "must prioritize this initiative to ensure comprehensive [redacted]

While DER, in its 2016 ROE for Fannie Mae, included [redacted] raised by Fannie Mae's Internal Audit function and external consultant relating to Fannie Mae's management of cybersecurity risks, DER completed no supervisory activities relating to those controls during the 2016 supervisory cycle. Its failure to complete any of those activities, and determine whether findings should issue, creates a significant risk that Fannie Mae's board of directors will be deprived of information necessary to execute the cyber risk management responsibilities delegated to it by FHFA.

FHFA's Continued Focus on Supervision of Cybersecurity at the Enterprises

In its PAR issued in November 2016, FHFA again recognized that threats to information security and the frequency and sophistication of cyber attacks are an area of focus for all financial service regulators, and stated that "FHFA continues to adjust its supervision activities to address these evolving risks." Notwithstanding FHFA's acknowledgement that cybersecurity continues to present a significant risk, DER's record of its supervisory activities during 2016 demonstrates that its actions fall short of FHFA's representations.

FINDINGS

1. DER Failed to Link its Planned Supervisory Activities to Identified Cybersecurity Risks as Required

The *FHFA Examination Manual* and 2013-DER-OPB-03.1 require that DER's written annual supervisory strategy for each Enterprise form a bridge between the significant risks and supervisory concerns identified in the risk assessment and the planned supervisory activities and that its annual supervisory plan link the objectives of planned supervisory activities to document risks. We found that DER did not meet these requirements.

While its annual Supervisory Strategy for Fannie Mae identified four broad areas of operational risk relating to cybersecurity management at Fannie Mae, we determined that it contained no information on the planned supervisory approach to address these four high-level risks. Similarly, we found that DER did not establish a link between the objectives of the planned supervisory activities relating to cybersecurity management at Fannie Mae and the risks in the Operational Risk Assessment. We could not determine whether the planned supervisory activities addressed the risks DER considered the most critical because DER did not identify which cyber risks were the most critical in the Operational Risk Assessment.

2. DER Failed to Complete Any Planned Supervisory Activities Related to Cybersecurity Risks at Fannie Mae, Except for Three Ongoing Monitoring Activities Related to Fannie Mae's Remediation of MRAs

DER's annual supervisory plan set forth four supervisory activities involving cybersecurity risks at Fannie Mae for the 2016 examination cycle: two targeted examination and two ongoing monitoring activities. It also identified three additional ongoing monitoring activities relating to Fannie Mae's remediation of MRAs. As a result of DER's mid-year revision to its 2016 supervisory plan, the four supervisory activities were addressed as follow: one targeted examination was descoped, another was converted to an ongoing monitoring activity, and the two ongoing monitoring activities were also descoped. According to the August 8, 2016, internal memorandum, all of DER's supervisory activities had been "descoped due to the limited time available due to the focus on MRA closure."

According to a DER official, DER considers a supervisory activity to be completed once the supervisor signs off on the relevant examination documentation. Applying this criteria, we found that the eClearance entries showed that an examination manager signed off on three of the four non-MRA ongoing monitoring activities relating to Fannie Mae's cybersecurity risks in May and June 2017, well after the ROE for the 2016 examination cycle issued on March 3,

2017. As of September 2017, eClearance entries reflect that the remaining targeted examination had not been completed.

DER's failure to complete planned supervisory activities for Fannie Mae has been a reoccurring problem. In an audit issued last year, we found that DER completed less than half of its 2012 through 2015 planned targeted examinations for Fannie Mae and did not complete many of its planned targeted examinations for each supervisory cycle prior to the issuance of the respective cycle's ROE. In that report, we recommended that DER assess whether it had a "sufficient complement of qualified examiners to conduct and complete those examinations rated by DER to be of high-priority within each supervisory cycle and address the resource constraints that have adversely affected DER's ability to carry out its risk-based supervisory plans." In its response dated September 22, 2016, DER did "not agree that current staffing levels have adversely affected DER's ability to meet its supervisory responsibilities."

Six weeks prior to issuing that response, DER staff reported in a written memorandum that DER descoped all operational risk (which includes information technology) supervisory activities "due to the limited time available due to the focus on MRA closure." DER staff explained in that memo that "a number of staffing and structural changes in 2016…directly impacted execution of the 2016 examination plan," and reported that all ongoing monitoring activities and targeted examinations were "descoped due to the limited time available due to the focus on MRA closure." We found that DER did not complete any of its planned Fannie Mae's cybersecurity supervisory activities, other than those related to MRA remediation, during the 2016 examination cycle. DER's failure to complete any of its planned supervisory activities relating to Fannie Mae's cybersecurity risks during 2016, a stated key objective of FHFA's supervision during 2016, provides additional cause for concern about the soundness of DER's supervisory practices and strategy.

3. The 2016 ROE Contained Conclusions by DER that Were Not Based on Completed Examination Work

According to FHFA, the ROE communicates to the board of directors of a regulated entity substantive examination conclusions, findings (when applicable), and the composite and component ratings. Because DER completed none of its planned supervisory activities for the 2016 supervisory cycle during that cycle (or before the ROE issued on March 3, 2017), it had no findings related to its 2016 examination work on cybersecurity to report in the section of the ROE titled "Information Security and Cyber-Security."

DER instead discussed assessments on Fannie Mae's cybersecurity risks provided from two Fannie Mae-related sources. While DER reported in the ROE that both Fannie Mae's Internal Audit and its external consultant identified [redacted] relating to Fannie Mae's management of cybersecurity risks, it was unable to provide a supervisory perspective on

those issues because it had not completed any of its planned supervisory activities regarding Fannie Mae's management of cybersecurity risks. The one conclusion included in this section of the ROE was not tethered to examination work completed during the 2016 cycle. DER's determination to include that unvetted conclusion was contrary of its own requirements.

In a different section of the ROE, DER included one observation and one adverse finding relating to Fannie Mae's management of cybersecurity. We found no evidence that DER previously communicated this observation and finding to Fannie Mae, in writing, as required by DER-OPB-02.

DER officials have represented to us that no quality assurance review is required for ROEs because the underlying work reported in each ROE has already been subject to such review. Because DER failed to complete any of its supervisory activities relating to Fannie Mae's management of cybersecurity during the 2016 supervisory cycle, no quality assurance review was conducted for the cybersecurity-related conclusions and observation included by DER in this ROE, in derogation of DER's own requirements. Including supervisory observations and conclusions in a ROE that have not be subject to a quality control review increases the risk that DER will provide misinformation to the Enterprise.

4. DER's Failure to Complete Any Planned Supervisory Activities Relating to Fannie Mae's Management of Cybersecurity Risks Creates the Significant Risk that the Fannie Mae Board of Directors Will Be Deprived of Supervisory Information Necessary for it to Execute Management Responsibilities Delegated by FHFA

FHFA has delegated responsibility for oversight of general corporate matters to each Enterprise's board of directors, including oversight of the risk management program, which includes cyber risk. FHFA has supplemented its general governance standards with supervisory expectations for board oversight and monitoring of an Enterprise's cyber risk management program set forth in its AB 2014-05. FHFA has also directed that the board of each regulated entity is responsible for having policies in place to assure oversight of the Enterprise's risk management program and of "[t]he responsiveness of executive officers…addressing all supervisory concerns of FHFA in a timely and appropriate manner."[17]

While DER, in its 2016 ROE for Fannie Mae, included [redacted] raised by Fannie Mae's Internal Audit function and external consultant relating to Fannie Mae's management of cybersecurity risks, DER completed no supervisory activities relating to those controls during the 2016 supervisory cycle. Its failure to complete any of those activities and determine whether findings should issue creates a significant risk that Fannie Mae's board

[17] 12 C.F.R. § 1239.4(c)(1), (3).

of directors will be deprived of information necessary to execute the cyber risk management responsibilities delegated to it by FHFA.

CONCLUSION

The Enterprises store, process, and transmit significant amounts of financial data and personally identifiable information in connection with their mission to support the secondary mortgage market. FHFA recognizes that cybersecurity is a significant risk for both Enterprises in light of the frequency and sophistication of attacks on information technology systems of financial institutions. In its 2015 PAR, the Agency advised: "A key objective of FHFA's supervisory work will continue to be the effective oversight of how each Enterprise manages cyber risks and addresses vulnerabilities." During the 2016 supervisory cycle, the Deputy Director, DER, underscored the importance of cybersecurity examinations for the supervision of financial institutions. In her March 2016 response to an OIG evaluation report, she stated: "cybersecurity is a critical area for risk management by financial institutions and should continue to be a principal focus for federal financial regulators."

We performed this audit to assess two objectives. First, we sought to determine whether the supervisory activities planned by DER relating to Fannie Mae's cybersecurity risks for the 2016 examination cycle addressed the cybersecurity risks highlighted in its risk assessment and supervisory strategy. We found that DER did not establish such a link in its supervisory planning documents to the risks it identified in its Operational Risk Assessment. We also could not determine whether the planned supervisory activities addressed the risks DER considered the most critical because DER did not identify which risks were the most critical in either the Operational Risk Assessment or the Supervisory Strategy.

Second, we sought to determine whether the four planned supervisory activities relating to Fannie Mae's cybersecurity management for the 2016 examination cycle were completed during that cycle. We found that DER did not complete any of its supervisory activities relating to Fannie Mae's cybersecurity risks planned for the 2016 examination cycle during that cycle. However, DER did complete three ongoing monitoring activities relating to Fannie Mae's remediation of prior MRAs.

We cannot reconcile FHFA's representations in its 2015 PAR that "effective oversight of how each Enterprise manages cyber risks and addresses vulnerabilities" would be a "key objective of FHFA's supervisory work" during 2016 with DER's inability to complete its four planned supervisory activities relating to cybersecurity during the 2016 examination cycle.

Because DER completed no planned supervisory activities during 2016 relating to management of cybersecurity risk by Fannie Mae (other than closing MRAs issued in prior years), it had no findings to report in the section of the 2016 ROE titled "Information Security and Cyber-Security" relating to information security and cybersecurity. Lacking supervisory information relating to management of information security risks to report in this ROE, DER

summarized the conclusions reached by Fannie Mae's Internal Audit function and by a contractor retained by Fannie Mae to perform a cyber risk assessment. There is a significant risk that DER's inability to complete any of its supervisory activities relating to Fannie Mae's management of its cybersecurity risks and reliance on conclusions reached by Fannie Mae's Internal Audit and its contractor deprives Fannie Mae's board of directors with information necessary to execute the cyber risk management responsibilities delegated to it by FHFA.

RECOMMENDATIONS

To address the shortcomings identified in this audit, we recommend that FHFA:

1. Assess whether DER has a sufficient complement of qualified examiners to conduct and complete those examinations rated by DER to be of high-priority within each supervisory cycle and address the resource constraints that have adversely affected DER's ability to carry out its risk-based supervisory plans. We made this recommendation in our 2016 audit discussed earlier and it remains open.

2. Reinforce through training and supervision of DER personnel, the requirements established by FHFA, and reinforced by DER guidance, for the risk assessment and supervisory planning process. Specifically:

    a. Ensure that the annual supervisory strategy identifies significant risks and supervisory concerns and explains how the planned supervisory activities to be conducted during the examination cycle address the most significant risks in the operational risk assessment.

    b. Ensure that supervisory activities planned during an examination cycle to address the most significant risks in the operational risk assessment are completed within the examination cycle.

3. Except for rare instances where DER has an urgent need to communicate significant supervisory concerns to an Enterprise board, ensure that all supervisory conclusions and findings reported by DER in the Enterprise's annual ROEs are based on completed work that has been previously communicated, when required, in writing to the Enterprise.

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 that cybersecurity is a significant area for risk management by the Enterprises and is a critical component of FHFA's supervision of the Enterprises. FHFA represented that it is working to improve its supervision protocols and processes to more effectively identify cybersecurity risks and address them in DER's examination activities. While FHFA disagreed with various statements in the draft report, it agreed with one recommendation and partially agreed with the other two recommendations. Its planned corrective actions are responsive to all of our recommendations.

OBJECTIVE, SCOPE, AND METHODOLOGY .....

We conducted this audit to assess (1) whether DER's planned supervisory activities relating to Fannie Mae's cybersecurity risks for the 2016 examination cycle tracked the cybersecurity risks highlighted in its risk assessment and supervisory strategy and (2) whether DER executed and completed these planned supervisory activities during the 2016 examination cycle.

To accomplish our objective, we reviewed the *FHFA Examination Manual.*

For Fannie Mae, we:

- Reviewed DER's risk assessments for the 2016 examination cycle to identify risks related to cybersecurity;
- Reviewed DER's supervisory strategy documents for the 2016 examination cycle to identify risks related to cybersecurity;
- Reviewed DER supervisory plan documents for the 2016 examination cycle to identify whether planned supervisory activities addressed the risks related to cybersecurity DER identified in the risk assessments and supervisory strategies;
- Interviewed DER personnel to gain an understanding of the supervision process and examination approach used to address Freddie Mac's cybersecurity risks;
- Reviewed DER's workpapers for the targeted examinations and ongoing monitoring related to cybersecurity performed during the 2016 examination cycle to determine whether required documents for each type of examination performed were completed and included in examination documentation in accordance with FHFA guidelines; and
- Reviewed the 2016 ROE to determine whether the results and conclusions of cybersecurity related supervisory activities were discussed.

We conducted this performance audit from March 2017 through September 2017 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 Complete Non-MRA Supervisory Activities Related to Cybersecurity Risks at Fannie Mae Planned for the 2016 Examination Cycle*

DATE: September 22, 2017

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

While we disagree with various statements in the Report and most of the findings, we agree that cybersecurity is a significant area for risk management by the Enterprises and is a critical component of FHFA's supervision of the Enterprises. FHFA is working to make improvements to our supervision protocols and processes to more effectively identify cybersecurity risks and address them in DER's examination activities. Consistent with these efforts, our responses to the specific recommendations are as follows.

Recommendation 1:

OIG recommends that FHFA assess whether DER has a sufficient complement of qualified examiners to conduct and complete those examinations rated by DER to be of high-priority within each supervisory cycle and address the resource constraints that have adversely affected DER's ability to carry out its risk-based supervisory plans. We made this recommendation in our 2016 audit discussed earlier and it remains open.

Management Response to Recommendation 1:

FHFA partially agrees with this recommendation. (i) By September 1, 2018, DER will assess the effectiveness of DER's Information Technology and Information Security Examinations branch, which was formed in 2017. (ii) By June 1, 2018, DER will determine whether to move staff or to request additional staffing resources to ensure consistency of 2019 examination coverage over cybersecurity risk. (iii) By September 1, 2018, DER will determine what 2019 cybersecurity-related training is needed for operational risk.

Recommendation 2:

OIG recommends that FHFA reinforce through training and supervision of DER personnel, the requirements established by FHFA, and reinforced by DER guidance, for the risk assessment and supervisory planning process. Specifically:

a. Ensure that the annual supervisory strategy identifies significant risks and supervisory concerns and explains how the planned supervisory activities to be conducted during the examination cycle address the most significant risks in the operational risk assessment.

b. Ensure that supervisory activities planned during an examination cycle to address the most significant risks in the operational risk assessment are completed within the examination cycle.

Management Response to Recommendation 2:

FHFA partially agrees with this recommendation. (i) By September 1, 2018, DER will provide training to all DER program staff (including Examiners-in-Charge and examination managers) on DER examination guidance and practices regarding the risk assessment and supervisory planning processes. (ii) Taken together, the risk assessment, examination plan, and supervisory strategy for each Enterprise will identify significant cybersecurity risks and describe how they will be covered in examination activities. (iii) By April 9, 2018, DER will conduct a review to document that all 2017 fieldwork was completed unless the examination activity was deferred or cancelled pursuant to an approved memorandum.

Recommendation 3:

OIG recommends that FHFA[,] except for rare instances where DER has an urgent need to communicate significant supervisory concerns to an Enterprise board, ensure that all supervisory conclusions and findings reported by DER in the Enterprise's annual ROEs are based on completed work that has been previously communicated, when required, in writing to the Enterprise.

Management Response to Recommendation 3:

FHFA agrees with this recommendation. (i) DER's current internal guidance does not describe the distinction between factual observations and supervisory views on risk exposures. By September 1, 2018, DER will amend its existing internal guidance to define the term "examination conclusions" to clarify what language must go through a QC review before inclusion in the Report of Examination (ROE). (ii) By January 31, 2018, DER will provide training to all examination staff on the provisions of DER-OPB-02, *Quality Control Reviews (June 23, 2016)*, with regard to what should be included in the 2017 ROEs.

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