REDACTED

Federal Housing Finance Agency
Office of Inspector General

FHFA Did Not Complete All Planned Supervisory Activities Related to Cybersecurity Risks at Freddie Mac for the 2016 Examination Cycle

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

Audit Report • AUD-2017-011 • September 27, 2017

AUD-2017-011

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 gulation (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 (hereafter, Deputy Director) also acknowledged the importance of cybersecurity for supervisors of financial institutions, observing in her March 2016 response to an Office of Inspector General (OIG) evaluation report that "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 Freddie Mac'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 a link between the objectives of the planned supervisory activities and the cybersecurity risks. However, we were able to link the cybersecurity risks identified in the Operational Risk Assessment to the objectives for three of the five non-MRA (Matter Requiring Attention) planned cybersecurity supervisory activities for this cycle. We were not able to link the stated objectives of two of the five planned supervisory activities to cybersecurity risks identified in DER's Operational Risk Assessment.

Second, we sought to determine whether the 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 Freddie Mac managed its cyber risk and addressed vulnerabilities. For the 2016 examination cycle, DER planned two targeted examinations at Freddie Mac, three ongoing monitoring activities relating to cybersecurity risks at Freddie

AUD-2017-011

September 27, 2017

Mac, and one other ongoing monitoring activity regarding Freddie Mac's effort to remediate a Matter Requiring Attention (MRA) issued by DER in a prior year. We found that DER did not complete one of its planned targeted examinations until after the 2016 ROE issued on March 10, 2017, and deferred the other. We also found that DER completed the three planned ongoing monitoring activities relating to cybersecurity risks at Freddie Mac as well as the planned MRA remediation ongoing monitoring activity.

DER's Operating Procedures Bulletin (OPB), DER-OPB-02, *Quality Control Reviews*, requires quality control reviews of all examination conclusions and findings before they are communicated to an Enterprise. According to DER, it does not conduct quality control reviews of the ROEs because all examination findings and conclusions undergo quality control reviews before they are incorporated in the ROEs. Notwithstanding DER's clear quality control requirements, DER included in the 2016 ROE the findings from an incomplete targeted examination that had not been subjected to a quality control review.

We make two 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 other recommendation. Its planned corrective actions are responsive to both 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 Fannie Mae's risk management of its cybersecurity risks. See *FHFA Failed to Complete Non-MRA Supervisory Activities Related to Cybersecurity Risks at Fannie Mae Planned for the 2016 Examination Cycle*, AUD-2017-010, available online at www.fhfaoig.gov/reports/auditsandevaluations.

Key contributors to this report were: Jackie Dang, IT Audit Director; Dan Jensen, Auditor-in-Charge; Terese Blanchard, Auditor; 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.

AUD-2017-011

September 27, 2017

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
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
PPI	Protected Personal Information
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 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 PAR 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

[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.

cyber 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 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 entities 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 .....

Cyber Risks Identified by DER in its Operational Risk Assessment for the 2016 Examination Cycle Can Be Linked to the Stated Objectives of Most But Not All of the Five Non-MRA Planned Supervisory Activities for That Cycle

Operational Risk Assessment for the 2016 Examination Cycle

DER's Operational Risk Assessment for the 2016 examination cycle reported that [redacted] The Operational Risk Assessment summarized DER's ongoing supervisory activities of Freddie Mac's [redacted]

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

In the Operational Risk Assessment, DER determined that Freddie Mac's operational risk remained [redacted] DER concluded that the direction of operational risk was [redacted]

Supervisory Strategy for the 2016 Examination Cycle

FHFA directs, in the *FHFA 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 2013-DER-OPB-03.1, *Supervisory Planning Process*, which directs that the annual supervisory strategy should include certain minimum information, including:

- 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.

Based on our comparison of the cybersecurity risks identified in DER's Operational Risk Assessment for the 2016 examination cycle for Freddie Mac to its 2016 Supervisory Strategy and the activities in the Supervisory Plan, we found that DER did not establish a link between the objectives of the planned supervisory activities and the risks in the Operational Risk Assessment. DER's 2016 Supervisory Strategy explained DER's supervisory approach for that year, which focused on four areas of operational risk relating to cybersecurity: [redacted]

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 vets 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.

DER's Supervisory Activities for the 2016 Examination Cycle

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

- Two targeted examinations,
- Three ongoing monitoring activities, and
- One other ongoing monitoring activity regarding Freddie Mac's efforts to remediate an MRA issued by DER in a prior year.[4]

We were able to link the cybersecurity risks identified in the Operational Risk Assessment to the objectives for three of the five non-MRA planned cybersecurity supervisory activities for this cycle. We were not able to link the objectives of two of the five non-MRA planned supervisory activities to risks identified in DER's Operational Risk Assessment.[5]

DER Completed Three of its Five Planned Supervisory Activities Related to Cybersecurity Risks at Freddie Mac during the 2016 Examination Cycle and the Planned Ongoing Monitoring to Oversee Freddie Mac's Remediation of an MRA Issued in a Prior Year

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 the planned

[4] At the mid-year update to the Supervisory Plan, DER added, as a change, an ongoing monitoring activity that was not in the initial plan for the examination cycle. The objectives for the other supervisory activities in the plan remained unchanged.

[5] In its technical comments, FHFA disputed our finding that the objectives for the two planned supervisory activities did not link to identified risks. For one planned supervisory activity, FHFA pointed to risks identified in a 2015 targeted examination as the foundation for the objective of the 2016 activity. For the other planned supervisory activity, FHFA claimed the risk was identified in the Operational Risk Assessment for 2016. We reviewed relevant documentation for the cited 2015 targeted examination and re-reviewed the Operational Risk Assessment and determined that the risks were not the same as those to be covered by the two planned supervisory activities in question.

supervisory activities relating to cybersecurity for Freddie Mac during the 2016 supervisory cycle.[6]

We found that DER did not complete either of the two planned targeted examinations during the 2016 supervisory cycle; one of the two, [redacted] was completed on April 17, 2017, and the other, [redacted] was deferred to the 2017 examination cycle.[7] We also found that DER completed the three planned ongoing monitoring activities (unrelated to MRA remediation) and none identified findings that were communicated to Freddie Mac. One ongoing monitoring activity related to DER's monitoring of Freddie Mac's remediation of an outstanding MRA was completed and DER issued a supervisory letter dated May 18, 2016, advising Freddie Mac that the MRA had been satisfactorily addressed.

While DER Did Not Complete Either Planned Targeted Examination Prior to the Issuance of the ROE for the 2016 Examination Cycle, it Reported Examination Findings from an Incomplete Targeted Examination in that ROE

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).

As explained earlier, DER did not complete the two targeted examinations planned for the 2016 supervisory cycle before the ROE issued for that cycle on March 10, 2017. DER-OPB-02 requires an independent quality control review be conducted and completed for examination conclusions, findings, and closures of MRAs before written communication of such conclusions, findings, and closures are communicated to the Enterprises. The quality reviews are done by staff outside of the team responsible for the written product. While FHFA's Supervision Directive 2013-01, *Quality Control Program for Examinations Conducted by the Division of Bank Regulation and the Division of Enterprise Regulation*,

[6] For purposes of this audit, we considered a targeted examination to be "completed" when DER issued a conclusion letter to Freddie Mac. Because DER did not issue a conclusion letter for completed ongoing monitoring activities without findings, we considered an ongoing monitoring activity to be "completed" when the fourth quarter memorandum prepared by DER examiners for that activity was approved by the risk manager.

[7] 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 examiner-in-charge (after consultation with the Deputy Director as warranted) and fully documented in the work papers. The decision, approved by the examiner-in-charge, to postpone this targeted examination to the 2017 examination cycle was made in October 2016 to allow sufficient time to gather details on Freddie Mac's internal testing results in this area. We consider this explanation reasonable.

instructed DER to perform quality control reviews of its ROEs prior to issuance, DER officials represented to us that no quality assurance review was required for ROEs because the underlying work reported in each ROE had been subjected to a quality assurance review. However, we found that the 2016 ROE issued by DER to Freddie Mac contained three recommendations[8] from an incomplete targeted examination involving cybersecurity before the results of that examination had completed DER's quality control review process. That targeted examination was not completed until April 17, 2017.[9]

[8] FHFA Advisory Bulletin AB 2017-01, *Classifications of Adverse Examination Findings*, establishes three classifications of adverse examination findings: MRAs, recommendations, and violations. Recommendations are advisory in nature and suggest changes to a policy, procedure, practice, or control that supervision staff believes would improve, or prevent deterioration in, condition, operations, or performance. Implementation is discretionary, although FHFA expects the Enterprise to implement recommendations unless the Enterprise can demonstrate through a reasoned assessment that the recommended action is unwarranted or is likely to be detrimental to condition, operations, or performance.

[9] DER-OPB-02, *Quality Control Reviews*, requires an independent quality control review of documentation for examination conclusions, findings, and closures of MRAs before written communication of such conclusions, findings, and closures to the Enterprises. The quality reviews are done by staff outside of the team responsible for the written product. DER has represented to us that no quality control review is required for ROEs because the underlying work reported in each ROE has been subjected to such review. *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).

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 Freddie Mac identified broad areas of operational risk relating to cybersecurity management at Freddie Mac, we found that DER did not establish a link between the objectives of the planned supervisory activities relating to cybersecurity management at Freddie Mac and the risks in the Operational Risk Assessment.

2. 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: substantive examination conclusions, findings (when applicable), and the composite and component ratings. We found that the Freddie Mac 2016 ROE contained [redacted] that was not completed, quality control reviewed, or communicated to the Enterprise until after the ROE issued. Including supervisory observations and conclusions in a ROE that have not been subjected to a quality control review increases the risk that DER will provide misinformation to the Enterprise.

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 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 Freddie Mac'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.

Second, we sought to determine whether the planned supervisory activities relating to Freddie Mac's cybersecurity management for the 2016 examination cycle were completed during that cycle. We found that DER did not complete either of the two planned targeted examinations during the 2016 supervisory cycle; one was completed after the Freddie Mac ROE issued but was discussed in the ROE before the targeted examination results underwent a quality control review and were reported to the Enterprise, and the other was deferred to 2017. DER did complete its planned 2016 ongoing monitoring activities within the 2016 examination cycle, including an MRA remediation activity.

RECOMMENDATIONS

In a companion report issued today, *FHFA Failed to Complete Non-MRA Supervisory Activities Related to Cybersecurity Risks at Fannie Mae Planned for the 2016 Examination Cycle* (September 27, 2017) (AUD-2017-010), we included the following recommendations that apply with equal force to address the findings identified in this report. We recommend that FHFA:

1. 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, 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.

2. 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 report, it agreed with one recommendation and partially agreed with the other recommendation. Its planned corrective actions are responsive to both of our recommendations.

OBJECTIVE, SCOPE, AND METHODOLOGY

We conducted this audit to assess (1) whether DER's planned supervisory activities relating to Freddie Mac'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 Freddie Mac, 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 Did Not Complete All Planned Supervisory Activities Related to Cybersecurity Risks at Freddie Mac 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 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, 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.

Management Response to Recommendation 1:

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.

Recommendation 2:

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 2:

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