REDACTED

Federal Housing Finance Agency
Office of Inspector General

FHFA Followed OMB Guidance in Implementing its Enterprise Risk Management Program But its 2020 Risk Profile Failed to Identify a Significant Action Underway to Address Acknowledged Supervision Risk

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

Audit Report • AUD-2021-004 • March 17, 2021

AUD-2021-004

March 17, 2021

Executive Summary

The Federal Housing Finance Agency (FHFA) is charged by the Housing and Economic Recovery Act of 2008 with the supervision of Fannie Mae and Freddie Mac (together, the Enterprises), any affiliate of the Enterprises, and the Federal Home Loan Banks (collectively, the regulated entities). Its mission as a federal financial regulator includes ensuring the safety and soundness of its regulated entities so that they serve as a reliable source of liquidity and funding for housing finance and community investment. Since 2008, FHFA has also served as conservator of the Enterprises.

Enterprise Risk Management (ERM) is a process that allows management to identify and understand the combined impact of external and internal risks, rather than addressing the risks within silos. In July 2016, the Office of Management and Budget (OMB) issued implementing guidance for ERM in its Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (Circular A-123 or the Circular) "to ensure Federal managers are effectively managing risks an agency faces toward achieving its strategic objectives and arising from its activities and operations."

We performed this audit to determine whether FHFA has implemented an ERM program that adheres to ERM guidance in Circular A-123, as adopted by FHFA. The audit focused on FHFA's ERM activities from inception in January 2017 through September 30, 2020 (review period).

We found that FHFA followed the guidance in Circular A-123 for its ERM program and prepared risk profiles for each year of the review period. These risk profiles addressed the components required by Circular A-123. However, FHFA did not include in its 2020 Annual Risk Profile a known significant action underway by the Agency to address identified residual risk in its Supervision program: it did not address an "organizational optimization Blueprint" project that was undertaken to ensure that FHFA "has the optimal workforce, infrastructure, and organization to carry out its supervisory mission in a post-conservatorship environment." FHFA's projected dates for deliverables from this project have slipped. In addition, we found that FHFA's ERM program was not supported by written policies and procedures.

We make two recommendations to address the identified shortcomings. In a written management response, FHFA agreed with our recommendations.

This report was prepared by James Lisle, Audit Director; April Ellison, Auditor-in-Charge; and Michael Rivera, Auditor; with assistance from Abdil Salah, Assistant Inspector General for Audits; and Bob Taylor, Senior

AUD-2021-004

March 17, 2021

Advisor. We appreciate the cooperation of FHFA staff, as well as the assistance of all those who contributed to the preparation of this report.

This report has been distributed to Congress, the Office of Management and Budget, and others and will be posted on our website, www.fhfaoig.gov, and www.oversight.gov.

Marla A. Freedman, Senior Audit Executive /s/

TABLE OF CONTENTS

ABBREVIATIONS

Circular A-123 or the Circular	Office of Management and Budget Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control
COO	Chief Operating Officer
DER	Division of Enterprise Regulation
ECIC	Executive Committee on Internal Controls
Enterprises	Fannie Mae and Freddie Mac
ERM	Enterprise risk management
ERM Playbook	Playbook: Enterprise Risk Management for the U.S. Federal Government
FHFA	Federal Housing Finance Agency
FMFIA	Federal Managers' Financial Integrity Act of 1982
GAO	Government Accountability Office
Green Book	Standards for Internal Control in the Federal Government
OBFM	Office of Budget and Financial Management
OIG	Federal Housing Finance Agency Office of Inspector General
OMB	Office of Management and Budget
RMC	Risk Management Council
RMWG	Risk Management Working Group

BACKGROUND

Federal Managers' Financial Integrity Act of 1982 Underpins Internal Control in the Federal Government, Including Enterprise Risk Management

As acknowledged by FHFA in its Performance and Accountability Report 2020, its management is responsible for establishing and maintaining effective internal control and financial management systems that meet the objectives of the Federal Managers' Financial Integrity Act of 1982 (FMFIA). In accordance with FMFIA, the Government Accountability Office (GAO) prescribed standards for internal control that Federal agencies, including FHFA, are to follow in its *Standards for Internal Control in the Federal Government* (Green Book).[1] Relevant to this audit are two principles for the risk assessment component of internal control set forth in the Green Book:

- Agency management should define objectives clearly to enable the identification of risks and define risk tolerances (Principle 6); and
- Agency management should identify, analyze, and respond to risk related to achieving the defined objectives (Principle 7).

Aligned with these two principles is the direction from OMB to federal agencies to conduct ERM in order to identify and understand the combined impact of external and internal risks, rather than addressing the risks within silos. OMB issued implementing guidance in Circular A-123 for ERM in July 2016 "to ensure Federal managers are effectively managing risks an agency faces toward achieving its strategic objectives and arising from its activities and operations."[2] To that end, the Circular required executive agencies to implement an ERM capability beginning in fiscal year 2017. OMB encouraged non-executive agencies of the Federal government to adopt the Circular. FHFA adopted the Circular, with some exceptions.[3]

[1] The current revision to the Green Book, GAO-14-704G, *Standards for Internal Control in the Federal Government*, was issued in September 2014.

[2] Circular A-123 provides guidance to Federal Managers on improving the accountability and effectiveness of Federal programs and operations by identifying and managing risks, and establishing requirements to assess, correct, and report on the effectiveness of internal controls. The Circular is issued under the authority of FMFIA.

[3] FHFA officials reported to us that FHFA does not follow (1) the deadlines prescribed by the Circular for its annual risk profile, (2) the requirement to submit its risk profile to OMB, and (3) the requirement to include a fraud objective in the Agency's risk profile because FHFA officials asserted that fraud risk for FHFA operations is low and no residual fraud risks were identified. These exceptions are not documented in writing.

Circular A-123 Requirements and Best Practices for ERM in the Federal Government

Circular A-123 includes requirements and best practices for implementing ERM. Among other things, it provides guidance for an ERM governance structure and requires that agencies maintain a risk profile.[4]

ERM Governance Structure

Circular A-123 states that agencies may use a Risk Management Council (RMC) to oversee the establishment of the agency's risk profile, conduct regular assessments of risk, and develop appropriate risk response(s). Further, the Circular states that an effective RMC will include senior officials for program operations and mission-support functions to help ensure those risks are identified that have the most significant impact on the mission outcomes of the agency. The Circular also states that should an agency choose to use an RMC, the council should be chaired by the agency Chief Operating Officer (COO) or a senior official with responsibility for the enterprise.

ERM Model

The Circular recognizes that many approaches can be taken to implement ERM but advises that the following elements should be included:

- Establish the Context – understand and articulate the internal and external environments of the organization.
- Initial Risk Identification – use a structured and systematic approach to recognize where the potential for undesired outcomes or opportunities can arise.
- Analyze and Evaluate Risks – consider the causes, sources, probability of the risk occurring, and the potential positive or negative outcomes, then prioritize the results of the analysis.
- Develop Alternatives – systematically identify and assess a range of risk response options guided by risk appetite.
- Respond to Risks – make decisions about the best option(s) among alternatives, and then prepare and execute the selected response strategy.

[4] Agencies subject to this Circular have some flexibility in the governance and implementation of their ERM process.

- Monitor and Review – evaluate and monitor performance to determine whether the implemented risk management options achieved the stated goals and objectives.

- Continuous Risk Identification – use an iterative process, occurring throughout the year, to include surveillance of leading indicators of future risk from internal and external environments.

Components of a Risk Profile

Circular A-123 directs covered agencies to maintain a risk profile, and FHFA has agreed to prepare and maintain one. A risk profile is a prioritized inventory and assessment of the most significant risks facing the agency. The primary purpose of a risk profile is to provide a thoughtful analysis of the risks that may interfere with achievement of an agency's strategic objectives and to identify appropriate options for addressing significant risks. According to Circular A-123, the ERM process should include a process for considering the agency's risk appetite[5] and tolerance levels.[6]

According to Circular A-123, risk profiles should include the following components: (1) identification of objectives, (2) identification of risk, (3) inherent risk assessment,[7] (4) current risk response, (5) residual risk assessment,[8] and (6) proposed risk response.

ERM Maturity Model

OMB, in Circular A-123, recognizes that Federal agencies have diverse missions and are at different levels of maturity in terms of their capacity to fully implement ERM. The Circular states that agencies should develop a maturity model approach to the adoption of an ERM framework and that an agency's approach for developing risk profiles and implementing ERM should be refined and improved each year. This guidance recognizes that not all components of an ERM process may be operational in the initial years, and agency leadership has flexibility to set priorities for implementation. A document titled Playbook: Enterprise Risk Management for the U.S. Federal Government (ERM Playbook) provides examples of

---

[5] Risk appetite is the broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision. It is established by the organization's most senior level leadership and serves as the guidepost to set strategy and select objectives.

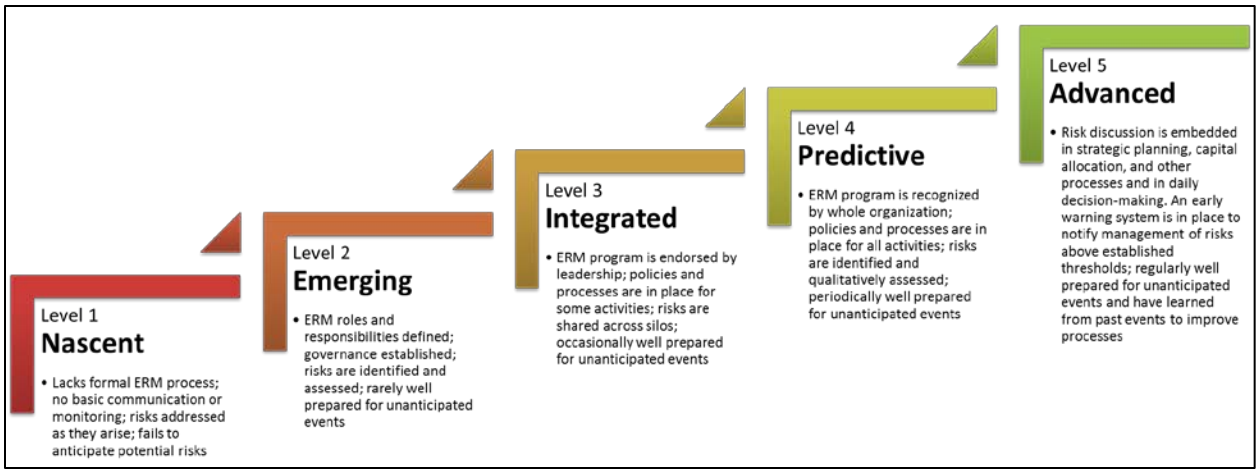
[6] Risk tolerance is the acceptable level of variance in performance relative to the achievement of objectives. It is generally established at the program, objective, or component level. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite.

[7] Inherent risk is the exposure arising from a specific risk before any action has been taken to manage it beyond normal operations.

[8] Residual risk is the exposure remaining from an inherent risk after action has been taken to manage it, using the same assessment standards as the inherent risk assessment.

ERM maturity models.[9] A maturity model from this guidance has been adopted by FHFA and is shown below:

FIGURE 1. ENTERPRISE RISK MANAGEMENT MATURITY MODEL (ADOPTED BY FHFA)



Source: ERM Playbook and FHFA ERM documents.

For fiscal years 2017 and 2018, FHFA assessed its ERM program maturity as "Emerging" (Level 2). The Agency has not assessed the maturity of its program since then.

FHFA's Executive Committee on Internal Controls, Committee Charter

Originally approved in March 2009, and most recently revised in April 2020, FHFA set forth the Committee Charter for its Executive Committee on Internal Controls (ECIC or Committee). The ECIC serves as the governance body for the Agency's implementation of Circular A-123 and the Green Book. Consistent with the Circular, FHFA's COO serves as the ECIC Chair and FHFA's Chief Financial Officer serves as the Vice-Chair. The ECIC provides leadership and structure for FHFA's ERM activities. Through this Charter, the ECIC established a cross-functional working group, the Risk Management Working Group (RMWG), to support the Committee.[10] The Office of Budget and Financial Management (OBFM), within FHFA's Office of the COO, is responsible for coordinating the RMWG's efforts.

[9] Issued by the Chief Financial Officers Council and the Performance Improvement Council in July 2016, the ERM Playbook provides guidance to help government departments and agencies meet OMB Circular A-123 requirements.

[10] Established in the ECIC Charter, the RMWG is a group of managers and staff, within FHFA, who assist in the development of the Agency's ERM framework. The group meets periodically to discuss the ERM framework, gathers input into potential risks facing the Agency, and vets ERM deliverables prior to ECIC's review.

FACTS AND ANALYSIS

FHFA's Documentation of its ERM Program Followed the Guidance in Circular A-123 But FHFA Failed to Identify a Significant Action Underway to Address Acknowledged Supervision Risk

Documents Establishing FHFA's ERM Program Met the Requirements in Circular A-123

Our review of the written risk profiles and other ECIC/RMWG documentation developed over the course of our review period found that FHFA's ERM program contained processes that addressed the elements of ERM described in Circular A-123. Specifically, FHFA, during the review period:

- Established the context – FHFA identified existing ERM guidance, established definitions for critical ERM concepts such as risk appetites and risk tolerances, and analyzed FHFA's internal and external environment.
- Initially identified risks – FHFA engaged in a process where it identified and prioritized risks in its respective divisions.
- Analyzed and evaluated the top risks – Using a standard methodology, FHFA assessed its top risks. This methodology included establishing the risk appetite and risk tolerance for each risk, identifying the existing controls in place to mitigate the risks, and prioritizing the top residual risks according to likelihood (probability of the risk occurring) and impact (the potential positive or negative outcomes).
- Developed alternatives – Through the ECIC, FHFA considered four alternatives to respond to risks: Accepted, Avoided, Reduced, or Shared.[11] FHFA either Accepted or Reduced each residual risk identified.
- Developed risk response actions – Through the ECIC, FHFA identified some specific risk response actions, the risk response "owners," and risk response target dates to mitigate residual risks that it determined to have a "Reduce" risk response.
- Monitored and reviewed identified risk response actions – FHFA instituted a process to obtain periodic status updates from risk "owners" on designated risk response

[11] According to FHFA: (1) for an Accepted risk, no action is taken; (2) for an Avoided risk, action is taken to stop the operational process causing the risk; (3) for a Reduced risk, action is taken to reduce the likelihood or impact of the risk; and (4) for a Shared risk, action is taken to transfer or share risks across the entity or with external parties.

actions. These updates were reported by way of a "dashboard" presented to the ECIC on a quarterly basis.[12]

- Continually identified risks – In accordance with the ECIC Charter, the RMWG/ECIC held periodic meetings to assess existing risks, identify new risks, and make updates to FHFA's Risk Profile.[13]

FHFA's Risk Profiles Addressed Components Required by Circular A-123

Consistent with Circular A-123, FHFA prepared an annual risk profile for each year of the review period. Each of FHFA's Annual Risk Profiles included risk categories covering both mission areas and operations (e.g., Supervision, Liquidity and Access, Conservatorship, Business Continuity, Human Capital, Financial Reporting, etc.).

The annual risk profiles addressed the major components of a risk profile, as described in the Circular. The annual risk profiles included a description of each identified inherent risk and the mission objective and performance target impacted by the risk, as well as an evaluation of FHFA's risk appetite and risk tolerance for the inherent risk. Further, the annual risk profiles listed existing controls (i.e., processes, procedures, and guidance) in place to mitigate the inherent risk; described and assessed any remaining residual risks based on likelihood (i.e., high, medium, or low) and impact (i.e., high, medium, or low); and described FHFA's risk response posture (i.e., Reduce or Accept) along with associated risk response actions, the owner of the risk response action, and a target completion date for most actions.

FHFA's 2020 Risk Profile Did Not Include a Known Significant Action Underway to Address Residual Risk for Supervision

We found that FHFA's 2020 Annual Risk Profile, finalized on September 23, 2020, did not include a significant action underway by the Agency to address identified residual risk in its Supervision program. In its 2020 Annual Risk Profile, FHFA identified as its Supervision risk:

[redacted]

[12] These dashboards list each residual risk that has been identified on the Risk Profile, FHFA's response to the risk, its response action items to reduce the residual risk, and the status/estimated completion date.

[13] We found that FHFA's ECIC has been established consistent with Circular A-123. Specifically, FHFA's ECIC is comprised of senior-level officials in program and mission-support functions and is chaired by the COO.

The 2020 FHFA Annual Risk Profile also listed risk response actions designed to reduce the recognized Supervision risk, the "owner" of that response action (responsible office), and the target completion date of the response action. The only risk response actions listed in the 2020 Profile for the Supervision residual risk were updating internal or external guidance by the Division of Enterprise Regulation (DER) and the Division of Federal Home Loan Bank Regulation, and updating the FHFA Examination Manual by DER; all those risk response actions were marked "complete."[14] As a result, the Profile indicates that there are no Supervision risk response actions currently pending and incomplete.

The 2020 FHFA Annual Risk Profile for Supervision risk did not identify an undertaking by FHFA in 2020. We reported in February 2020 that, despite prior commitments, FHFA had not implemented a systematic workforce planning process to determine whether enough qualified examiners are available to assess the safety and soundness of the Enterprises.[15] We found that the failure to adopt systematic workforce planning, and DER's persistent failure to complete targeted examinations in the cycle for which they were planned, called into question its supervisory capacity. We also reported in a March 2020 evaluation that despite FHFA's recognition of significant risks associated with the Enterprises' high-risk models, its examination of those models over a six-year period has been neither rigorous nor timely.[16] During our evaluation, DER officials asserted that budgetary constraints and limited resources contributed to DER's inability to conduct more targeted examinations of Enterprise high-risk models. We found that DER's failure to conduct systematic workforce analyses for model risk deprived DER of data necessary to determine, among other things, the number of qualified model examiners needed. To address these questions about its supervisory capacity, we

[14] We have not assessed whether the newly issued internal and external guidance provides a substantive update from prior guidance.

[15] *See* OIG, *Despite Prior Commitments, FHFA Has Not Implemented a Systematic Workforce Planning Process to Determine Whether Enough Qualified Examiners are Available to Assess the Safety and Soundness of Fannie Mae and Freddie Mac* (Feb. 25, 2020) (AUD-2020-004) (online ***here***).

[16] *See* OIG, *Despite FHFA's Recognition of Significant Risks Associated with Fannie Mae's and Freddie Mac's High-Risk Models, its Examination of Those Models Over a Six Year Period Has Been Neither Rigorous nor Timely* (Mar. 25, 2020) (EVL-2020-001) (online ***here***).

recommended that FHFA direct DER to develop and implement a systematic workforce planning process within 12 months that aligns with Office of Personnel Management guidance.

In response to recommendations made in both reports, the Agency informed us on June 30, 2020, that it had engaged a contractor to prepare an "organizational optimization Blueprint" to ensure that FHFA "has the optimal workforce, infrastructure, and organization to carry out its supervisory mission in a post-conservatorship environment." The scope of the consultant's engagement included assessing FHFA's existing and future workforce needs relative to a "best practice definition of a world class regulator." FHFA management stated that the Blueprint project should achieve a substantially similar result to our recommendation, and the Agency agreed to review the Blueprint and determine the need for additional workforce planning specific to DER. However, we found that neither the "organizational optimization Blueprint" nor its risk response owners or risk response target dates were identified in FHFA's 2020 Annual Risk Profile for Supervision risk.[17]An FHFA official explained to us that the identification of actions related to the "organizational optimization Blueprint" was deferred until 2021.[18] As we cautioned in our March 2020 report, FHFA Faces a Formidable Challenge: Remediating the Chronic and Pervasive Deficiencies in its Supervision Program Prior to Ending the Conservatorships of Fannie Mae and Freddie Mac, remediating the

[17] In August 2020, FHFA informed us that based on its then current project plan for the Blueprint, it would provide us with certain project deliverables by October 30, 2020. This date has slipped. On January 22, 2021, we were told by an FHFA official that the project deliverables were still under management review. The FHFA official also could not give us a date when the deliverables would be made available.

[18] The FHFA official also asserted that the organizational optimization Blueprint was identified in another section of FHFA's 2020 Annual Risk Profile: Strategic Residual Risk. In our view, the reference to this Blueprint in another section of the risk profile was so obscure that most users would not make this connection.

The identified Strategic Residual Risk was:

[redacted]

FHFA identified four risk response actions to reduce this residual risk: (1) Legislative authority – work with Congress to strengthen FHFA's powers, (2) PSPA – work with the Department of the Treasury on any required changes to the Senior Preferred Stock Purchase Agreements with the Enterprises, (3) [redacted], and (4) "Organizational – To be developed and longer term plans are developed." Minutes from a September 2020 RMWG meeting to develop the 2020 FHFA Risk Profile provide some additional context to this fourth risk response action item – "organization[al] optimization project underway, but organization changes are longer term item" – suggesting the item related to the "organizational optimization Blueprint." That said, the owner identified for all four risk response actions was FHFA's Division of Resolutions and target dates were "TBD." In our view, the reference to "Organizational" is too vague to be considered a specific risk response action to FHFA's identified supervision risk. Further, it makes no sense that this risk response action would be assigned to the Division of Resolutions – the division assigned to oversee the conservatorship – because the risk is a supervisory risk.

deficiencies identified by us and by FHFA before the Enterprises are released from conservatorship will demand disciplined project management, including the establishment of clear roles and responsibilities, work product deliverables, milestones, and specific timelines.[19] To date, FHFA has not put into place disciplined project management to implement the recommendations from the Blueprint project, which increases the risk that the necessary remediation will not occur in a timely manner.[20]

FHFA's ERM Program Has Not Been Supported by Written Policies and Procedures

We found that the ECIC Charter provides guidance for the governance of FHFA's ERM program, and OBFM presentation materials prepared for RMWG and ECIC meetings describe the ERM program's mission and objectives, identify planned activities for the year, define risk appetite and tolerance, and provide an overview of the methodology used to develop FHFA's risk profile. However, we also found that FHFA's ERM program was not supported by written policies and procedures. For example, while the presentation materials described FHFA's initial risk identification and assessment process, there were no policies or procedures for continuous risk identification and assessment, development and monitoring of risk responses, or documenting ERM program activities.

The Green Book notes that effective documentation assists in management's design of internal control by establishing and communicating the who, what, when, where, and why of internal control execution to personnel. It also provides a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel. An OBFM official acknowledged the benefits of developing written policies and procedures but also noted that OBFM prioritized developing the Agency's governance, framework, and risk profiles before developing policies and procedures.

FINDINGS

- FHFA's 2020 Risk Profile did not include a known significant action underway to address residual risk for Supervision.

[19] *See* OIG, *FHFA Faces a Formidable Challenge: Remediating the Chronic and Pervasive Deficiencies in its Supervision Program Prior to Ending the Conservatorships of Fannie Mae and Freddie Mac* (Mar. 30, 2020) (OIG-2020-002) (online ***here***).

[20] In a technical comment to a draft of this report, FHFA stated that in its Annual Performance Plan for Fiscal Year 2021, issued in December 2020, the Chief Operating Officer had been assigned to "[d]evelop an action plan to address improvement opportunities identified in FHFA's optimization study to further the development of a world-class supervision program." The target date for this action plan is June 30, 2021.

- FHFA's ERM program has not been supported by written policies and procedures.

CONCLUSIONS

FHFA followed the guidance in Circular A-123 for its ERM program and prepared risk profiles for each year of the review period. These risk profiles addressed the components required by Circular A-123. However, the risk response actions to its residual Supervision risk were incomplete and noted only projects which had been completed. Absent from the list was a significant action underway by the Agency to address identified residual risk in its Supervision program. FHFA's projected dates for deliverables from that project have slipped. As we cautioned previously, remediating deficiencies identified by us and by FHFA before the Enterprises are released from conservatorship will demand disciplined project management, including the establishment of clear roles and responsibilities, work product deliverables, milestones, and specific timelines. The lack of disciplined project management increases the risk that the necessary remediation will not occur in a timely manner. In addition, we found that FHFA's ERM program was not supported by written policies and procedures, increasing the risk that ERM processes would not be carried out in accordance with management's intent.

RECOMMENDATIONS

We recommend that FHFA:

1. Going forward, ensure Annual Risk Profiles include all significant risk response action items designed to reduce identified residual risks, such as FHFA's organizational optimization Blueprint project, along with identifying the owners of those risk response action items and target completion dates.

2. Develop written policies and procedures for its ERM program.

FHFA COMMENTS AND OIG RESPONSE

We provided FHFA an opportunity to respond to a draft report of this audit. FHFA provided technical comments on the draft report and those comments were considered in finalizing this report. FHFA also provided a management response, which is included in the Appendix of this report. In its management response, FHFA agreed with both recommendations and stated

that it will develop written policies and procedures for the ERM program by January 31, 2022. The procedures will include a review of the Annual Risk Profiles to confirm that significant action items to reduce the residual risks have been included, and that owners and target completion dates have been identified.

We consider FHFA's planned corrective actions responsive to our recommendations.

OBJECTIVE, SCOPE, AND METHODOLOGY

We performed this audit to determine whether FHFA has implemented an ERM program that adheres to ERM guidance in OMB Circular A-123, as adopted by FHFA. The audit focused on FHFA's ERM activities from inception in January 2017 through September 30, 2020 (review period).

To accomplish our objective, we:

- Reviewed the following sources of guidance on ERM:
  - OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 2016)
  - United States Chief Financial Officers Council and Performance Improvement Council, Playbook: Enterprise Risk Management for the U.S. Federal Government (July 2016)
  - GAO, *Standards for Internal Control in the Federal Government* (Sept. 2014)
  - The Council of the Inspectors General on Integrity and Efficiency (CIGIE), Inspectors General Guide to Assessing Enterprise Risk Management (Jan. 2020)
- Reviewed the ECIC Charter, RMWG mission statement, committee membership lists, meeting minutes, and ERM process presentation material, and interviewed FHFA management officials to gain an understanding of FHFA's ERM governance structure, practices, and process for implementing OMB Circular A-123.
- Determined whether FHFA adopted a maturity model approach to implementation of the ERM framework, and, if so, their view on FHFA's current stage of development and plans for advancing along the model.
- Reviewed RMWG meeting minutes for the review period and determined whether the RMWG:

- Met periodically to discuss the ERM framework, gather input into potential risks facing the Agency, vet ERM deliverables prior to ECIC review, and discuss ERM issues, as needed; and

- Worked with Agency stakeholders to (1) understand and document risk appetite and tolerance levels and (2) develop and maintain the Agency's risk profile, which includes identifying and evaluating risks to meet Agency objectives, developing, and implementing risk responses, and monitoring and reviewing risks.

- Reviewed the initial ERM Risk Profile and all subsequent ERM Risk Profiles prepared during the period 2017 to September 2020 to determine whether:

  - the risk profile, or changes to the risk profile, were approved in accordance with requirements established by the ECIC;

  - the risk profile used a format that addressed the major components recommended in OMB Circular A-123; and

  - the risk profile presented a prioritized list of risks.

- Reviewed each FHFA Strategic Plan, Annual Performance Plan, and Performance & Accountability Report for the review period and identified the population of strategic goals (objectives), operations objectives, reporting objectives, and compliance objectives in effect for each iteration of the ERM Risk Profile. Analyzed the risks included in the ERM Risk Profiles to determine whether risks were being assessed for all strategic goals, operations objectives, reporting objectives, and compliance objectives to include financial and fraud objectives.

  - For risks identified in the ERM Risk Profiles, determined whether the assessment elements (e.g., risk appetite, tolerance, impact, likelihood, risk response, and risk response action items) addressed the identified risk.

  - For each risk in the ERM Risk Profiles with risk response action items, reviewed the action item and determined whether the action was completed by the established target date.

We conducted this performance audit from September 2020 through March 2021 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 our 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 Freedman, Senior Audit Executive

FROM: Mark Kinsey, Chief Financial Officer MARK KINSEY Digitally signed by MARK KINSEY Date: 2021.03.11 10:18:34 -05'00'

SUBJECT: Draft Audit Report: *FHFA Followed OMB Guidance in Implementing its Enterprise Risk Management Program But its 2020 Risk Profile Failed to Identify a Significant Action Underway to Address Acknowledged Supervision Risk*

DATE: March 11, 2021

Thank you for the opportunity to above-referenced draft audit report (Report) by the Office of Inspector General. The objective of the audit was to determine whether the Agency has implemented an Enterprise Risk Management (ERM) program that adheres to the ERM guidance in the Office of Management and Budget (OMB) Circular A-123.

I am pleased that the audit concluded that the ERM program met the guidance in OMB Circular A-123 and the Risk Profiles addressed the required components. The response to the Report's recommendations are below:

Recommendation No. 1: *Going forward, ensure Annual Risk Profiles include all significant risk response action items designed to reduce identified residual risks, such as FHFA's organizational optimization Blueprint project, along with identifying the owners of those risk response action items and target completion dates.*

Recommendation No. 2: *Develop written policies and procedures for its ERM program.*

Management Response: FHFA agrees with the recommendations and will develop written policies and procedures for the ERM program by January 31, 2022. The procedures will include a review of the Annual Risk Profiles to confirm that significant action items to reduce the residual risks have been included, and that owners and target completion dates have been identified.

I would like to acknowledge the dedicated OIG staff that worked with FHFA during this audit.

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