Federal Housing Finance Agency
Office of Inspector General

Compliance Review of DBR's Assessment and Documentation of Critical Cybersecurity Controls in Examinations of the FHLBank System

Compliance Review • COM-2021-005 • June 15, 2021

COM-2021-005

June 15, 2021

Executive Summary

The Federal Housing Finance Agency (FHFA or Agency) is charged by the Housing and Economic Recovery Act of 2008 (HERA) with oversight of the Federal National Mortgage Association, the Federal Home Loan Mortgage Corporation, and the Federal Home Loan Bank (FHLBank) System (collectively, the regulated entities). The FHLBank System consists of 11 FHLBanks and the Office of Finance. Its mission is to provide reliable liquidity to member institutions to support housing finance and community investment. FHFA has identified that one priority for its supervisory activities is assessing the regulated entities' cybersecurity programs.

With an increasing number of cybersecurity incidents, including large-scale data breaches, affecting financial institutions of all sizes, institutions need adequate preventive and detective controls to mitigate the threat. Two such controls are vulnerability scans and penetration tests, which are applied to identify information security (IS) deficiencies and to determine if existing security measures in an entity's technology environment could be circumvented.

Our February 2016 audit found that FHFA's Division of Federal Home Loan Bank Regulation (DBR) examinations generally did not assess the design of the FHLBanks' vulnerability scans and penetration tests when evaluating those controls' operational effectiveness. We made two recommendations to address this shortcoming, both of which FHFA accepted: that the Agency (1) update its guidance to direct examiners to assess the design of the Banks' vulnerability scans and penetration tests when assessing the operational effectiveness of such controls; and (2) require examiners to document their assessments of the design of those scans and tests. In early 2017, the Agency updated its guidance to implement our recommendations and clarified that existing examiner documentation standards applied. We closed the recommendations in February 2017, based upon those actions.

In a 2019 compliance review, we found that DBR did not fully comply with the updated 2017 guidance for 11 out of 18 examinations (61%) in which DBR examiners evaluated the operational effectiveness of vulnerability scans and penetration tests. Based on this finding, we re-opened the recommendation that DBR should require examiners to document their design assessments of such scans and tests.

In March 2021, we initiated this compliance review to determine whether DBR documented assessments of the design of vulnerability scans and penetration tests when it examined the operational effectiveness of those controls during its examinations of FHLBanks and the Office of Finance

COM-2021-005

June 15, 2021

between April 1, 2019, and December 31, 2020 (review period). We found that, in every instance, DBR examiners documented such assessments. Based upon these findings, we are closing the re-opened recommendation that examiners document assessments of the design of vulnerability scans and penetration tests when examining the operational effectiveness of these controls.

This report was prepared by Karen E. Berry, Senior Investigative Counsel, and Patrice Wilson, Senior Investigative Evaluator. 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.

/s/

Brian W. Baker
Deputy Chief Counsel

TABLE OF CONTENTS

ABBREVIATIONS

Agency or FHFA	Federal Housing Finance Agency
DBR	FHFA Division of Federal Home Loan Bank Regulation
FHLBank	Federal Home Loan Bank
FHLBank System	The 11 FHLBanks and the Office of Finance
IS	Information Security
IT	Information Technology
IT Module	Information Technology Risk Management Program Module
OIG	FHFA Office of Inspector General
OSSE	DBR's Office of Safety and Soundness Examinations
Regulated Entities	The Federal National Mortgage Association, the Federal Home Loan Mortgage Corporation, and the FHLBank System
Review Period	April 1, 2019, to December 31, 2020

BACKGROUND

Overview of the FHLBanks' Cybersecurity Programs

The Federal Housing Finance Agency regulates the Federal Home Loan Bank System, which consists of the 11 FHLBanks and the Office of Finance, the FHLBanks' fiscal agent. The FHLBanks and the Office of Finance have established cyber risk management programs to mitigate the risks from potential cyber attacks. Vulnerability management is a critical component of an effective cyber risk management program and is defined as "the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities."

As part of their vulnerability management, the FHLBanks and the Office of Finance employ contractors to conduct vulnerability scans and penetration tests. Vulnerability scanning examines computers, systems, networks, and applications to identify security weaknesses. Penetration testing attempts to determine whether an attacker could successfully reach a specific database or system by circumventing existing controls.

Prior Reports Identified Deficiencies in DBR's Cyber Risk Management Programs

Federal financial regulators, including FHFA, consider cybersecurity to be among the foremost risks facing the banking and financial services industries. FHFA has identified that one priority for its supervisory activities is assessing the adequacy of cybersecurity programs of its regulated entities.

A 2016 Audit Found that DBR Examinations Did Not Include an Assessment of the Design of FHLBanks' Critical Cybersecurity Controls

In a 2016 audit, we explained that an examination of the operational effectiveness of information technology (IT) controls can only be reliable when examiners understand the design of those controls so that they can assess whether the controls would adequately mitigate risks. That audit looked at whether examiners who conducted 15 IT examinations of the FHLBanks during 2013 and 2014 assessed the design of vulnerability scanning and penetration testing performed by the FHLBanks' contractors.[1]

[1] OIG, *FHFA Should Improve its Examinations of the Effectiveness of the Federal Home Loan Banks' Cyber Risk Management Programs by Including an Assessment of the Design of Critical Internal Controls* (Feb. 29, 2016) (AUD-2016-001).

We found that, for 14 of the 15 examinations, the design of vulnerability scanning and penetration testing was not reviewed. We recommended that DBR implement two recommendations to address this shortcoming:

- Update its Information Technology Risk Management Program Module (IT Module)[2] to direct examiners to assess the design of the FHLBanks' vulnerability scans and penetration tests when assessing the operational effectiveness of such controls; and
- Require examiners to document their assessments of the design of the FHLBanks' vulnerability scans and penetration tests as part of their assessment of the operational effectiveness of such controls.

FHFA agreed with both recommendations.

In 2017, FHFA Began Requiring that Examiners Assess the Design of IT Controls

In January 2017, DBR updated its IT Module to require examiners, when assessing the operational effectiveness of vulnerability scans and penetration testing, to assess the design of those controls.

The IT Module identified four factors[3] for examiners to consider when assessing the design of vulnerability scans and penetration tests:

- Whether the parties that perform the vulnerability scans and penetration tests are sufficiently independent (i.e., not responsible for the design, installation, maintenance, and operation of any of the tested systems);
- Whether the institution's security risk assessment informs the frequency of the vulnerability scans and penetration tests;
- Whether the scopes and strategies of the vulnerability scans and penetration tests are commensurate with the institution's technology environment; and

[2] The *FHFA Examination Manual* contains individual examination modules that provide examination instructions to examiners on how to assess specific topics, business lines, and risk areas. Examination modules contain workprograms that help examiners assess the types of risk to which the regulated entity is exposed, the level of risk exposure, the direction of risk, and the quality of risk management practices. Each workprogram provides illustrative examples of worksteps and lines of inquiry the examiner could consider when completing the analysis required in the workprogram. Examiners must document their analysis, findings, and conclusions in the applicable workprogram.

[3] For ease of reference, we refer to this illustrative guidance as the "four factors" that relate to the design of protective measures, such as vulnerability scans and penetration tests.

- Whether the institution adequately addressed the findings from such vulnerability scans and penetration tests or has an adequate plan for remediation.

On February 17, 2017, we closed our recommendations based on DBR's responses and its inclusion of the new guidance in the IT Module.

In 2019, We Found that DBR Examiners Had Not Conducted Assessments of the Design of Vulnerability Scans and Penetration Tests as Required

A 2019 compliance review found that, for 11 of the 18 examinations (61%) in which DBR examiners evaluated the operational effectiveness of vulnerability scans and penetration tests, they did not fully comply with the revised guidance. Based on this finding, we re-opened the recommendation that DBR should require examiners to document their design assessments of vulnerability scans and penetration tests.

FINDING

In March 2021, we initiated this compliance review to determine whether DBR documented assessments of the design of vulnerability scans and penetration tests when it examined the operational effectiveness of such controls during its examinations of FHLBanks and the Office of Finance between April 1, 2019, and December 31, 2020. We found that, in every instance, DBR examiners documented such assessments.

DBR Examiners Conducted and Documented Assessments of the Design of Vulnerability Scans and Penetration Tests in 20 of 20 Examinations

We interviewed the DBR Deputy Director and the Associate Director of DBR's Office of Safety and Soundness Examinations (OSSE) to obtain an understanding of how the Agency implemented corrective actions in response to the reopened recommendation that DBR should require examiners to document their design assessments. The OSSE Associate Director stated that examiners' assessments of the design of vulnerability scans and penetration tests would be included either in IS or IT workprograms.

We determined that 20 examinations fell within our review period. For each of the 20 examinations, we reviewed the IS and IT workprograms for evidence that the examiner(s) had assessed the four factors pertaining to the design of vulnerability scans and penetration testing and documented their assessment.

We found that DBR conducted and documented such assessments for all 20 examinations. In every examination, the examiner assessed each factor separately and documented his or her analysis and conclusions in detail in the workprogram.

CONCLUSION

We initiated this compliance review to determine whether DBR documented assessments of the design of vulnerability scans and penetration tests when it examined the operational effectiveness of such controls during examinations of the FHLBanks and the Office of Finance conducted between April 1, 2019, and December 31, 2020. We reviewed 20 IT and IS workprograms completed during the review period. We found that DBR documented such assessments for all 20 examinations. In each examination, the examiner assessed each factor separately and documented his or her analysis and conclusions in detail in the workprogram. As a result, we are closing the re-opened recommendation that examiners document assessments of the design of vulnerability scans and penetration tests when examining the operational effectiveness of these controls.[4]

OBJECTIVE, SCOPE, AND METHODOLOGY

We initiated this compliance review in March 2021 to determine whether DBR conducted and documented assessments of the design of vulnerability scans and penetration tests when it examined the operational effectiveness of such controls during examinations of the FHLBanks and the Office of Finance conducted between April 1, 2019, and December 31, 2020. To do so, we reviewed DBR's scope memorandum for each examination to determine if the memorandum was approved during our review period. For the 20 examinations we identified to be within the scope of our compliance review, we then reviewed the completed IS and IT workprograms for evidence that the four factors pertaining to vulnerability scans and penetration testing were assessed and documented. We also interviewed the DBR Deputy Director and the DBR Associate Director of OSSE to obtain an understanding of how the

[4] The DBR Director said he would determine at the end of 2020 the appropriate frequency for assessing the design of vulnerability scans and penetration tests in DBR examinations where the FHLBank or the Office of Finance performed a vulnerability scan or penetration test since the prior examination. After work on this compliance review was completed, DBR officials reported to OIG that they are committing to assess vulnerability scans and penetration testing at every examination where DBR completes the IS workprogram. DBR stated that examiners will not be required to assess every one of the four factors. DBR clarified that the factors should serve as an overall guide to exam planning and that the examiners' coverage of the area should be "meaningful." OIG has not assessed these revised requirements.

Agency implemented corrective actions in response to the reopened recommendation that DBR should require examiners to document their design assessments.

We conducted our compliance review from March to April 2021 under the authority of the Inspector General Act of 1978, as amended, and in accordance with the Quality Standards for Inspection and Evaluation (January 2012), which were promulgated by the Council of the Inspectors General on Integrity and Efficiency.

We provided a draft of this report to FHFA for its review and comment.

APPENDIX: FHFA MANAGEMENT RESPONSE.....

Federal Housing Finance Agency

MEMORANDUM

TO: Brian W. Baker, Deputy Chief Counsel, Office of Inspector General

FROM: Andre D. Galeano, Deputy Director, Division of FHLBank Regulation (DBR)

ANDRE GALEANO Digitally signed by ANDRE GALEANO Date: 2021.06.14 08:48:02 -04'00'

SUBJECT: Draft Compliance Report: *Compliance Review of DBR's Assessment and Documentation of Critical Cybersecurity Controls in Examinations of the FHLBank System*

DATE: June 14, 2021

Thank you for the opportunity to respond to the Office of Inspector General (OIG) draft compliance report referenced above (Report). The Report covers certain cybersecurity assessments, vulnerability scans and penetration testing, and follows-up on an OIG 2019 compliance review.

I am pleased the OIG review found that examiners completed the assessments in all 20 examinations and the examiners documented their analysis and conclusions as detailed in the DBR work program. As a result, the OIG closed the re-opened recommendation from the 2019 compliance review.

We appreciate the work and professionalism of the OIG staff who worked with FHFA during this engagement. Please feel free to contact me with any questions or concerns.

cc: Chris Bosland
Kate Fulton
John Major
Richard Dalton

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