Federal Housing Finance Agency
Office of Inspector General

DBR's Quality Control Program Did Not Detect a Documentation Deficiency in Its Oversight of the FHLBank System's Information Security and Cybersecurity Risk Management

Audit Report • AUD-2026-003 • May 13, 2026

EXECUTIVE SUMMARY

PURPOSE

Each Federal Home Loan Bank (FHLBank) and the Office of Finance (collectively, the FHLBank System) relies heavily on information systems and other technology to conduct and manage business. The FHLBank System needs to protect the information technology assets and data under its control and manage cybersecurity risks - intentional and unintentional acts that may jeopardize the confidentiality, integrity, or availability of information technology assets and data.

As part of our ongoing oversight of the Division of Federal Home Loan Bank Regulation's (DBR) supervision of the FHLBank System, we performed this audit to assess whether DBR provided sufficient oversight of the FHLBank System's information security and cybersecurity risk management.

RESULTS

We determined that DBR provided sufficient oversight of the FHLBank System's information security and cybersecurity risk management. Specifically, we concluded that DBR designed examination guidance that provided examiners with the worksteps needed to provide such oversight. DBR examiners performed risk-based examinations of information security and cybersecurity risk management for the four examinations in our sample and generally documented their supervisory conclusions in accordance with DBR's workpaper standards. DBR also issued information security and cybersecurity-related Matters Requiring Attention (MRA); monitored the FHLBanks' progress to resolve deficiencies indentified in the MRAs; and closed MRAs, as appropriate, in accordance with its guidance. Overall, we found that DBR examiners were qualified and had the relevant experience to perform the Information Security Management workprogram examinations.

Although DBR provided sufficient oversight of the FHLBank System's information security and cybersecurity risk management, we found that DBR's quality control program did not detect and correct an instance in which the examiner analysis supporting a supervisory conclusion was not documented in the examination workpapers. The risk of incorrect supervisory conclusions increases when DBR's quality control program does not detect and correct examination workpaper deficiencies.

RECOMMENDATION

We made one recommendation to address our finding. In a written response, FHFA management agreed with our recommendation.

This report was prepared by James Lisle, Audit Director; Marco Uribe, Auditor-in-Charge; Jianxun Pan, Auditor; and Jeffrey Lloyd, Auditor; with assistance from Abdil Salah, Assistant Inspector General for Audits. We appreciate the cooperation of FHFA staff, as well as the assistance of all those who contributed to the preparation of this report. This report has been distributed to Congress, the Office of Management and Budget, and others and will be posted on our website, www.fhfaoig.gov, and www.oversight.gov.

James Hodge
Deputy Inspector General for Audits /s/

TABLE OF CONTENTS

EXECUTIVE SUMMARY 2

ABBREVIATIONS 5

BACKGROUND 6

Information Security and Cybersecurity Risk 6

Supervisory Expectations for the FHLBank's and the Office of Finance's Information Security and Cybersecurity Risk Management 6

Annual Examinations of the FHLBanks and the Office of Finance 8

DBR Guidance for Oversight of the FHLBank's and the Office of Finance's Information Security and Cybersecurity Risk Management 8

OBJECTIVE AND SCOPE 9

RESULTS 10

Finding: A Documentation Deficiency was Not Detected by DBR's Quality Control Program 11

FHFA COMMENTS AND OIG EVALUATION 12

APPENDIX I: METHODOLOGY 13

APPENDIX II: FHFA MANAGEMENT RESPONSE 18

ABBREVIATIONS

AB	Advisory Bulletin
DBR	Division of Federal Home Loan Bank Regulation
FHFA	Federal Housing Finance Agency
FHLBank	Federal Home Loan Bank
FHLBank System	FHLBanks and the Office of Finance
GAO	Government Accountability Office
MRA	Matter Requiring Attention
NIST	The National Institute of Standards and Technology
OIG	FHFA Office of Inspector General
OPB	Operating Procedure Bulletin
PMOS	FHFA's Prudential Management and Operations Standards
QCB	DBR Quality Control Branch

BACKGROUND

Each FHLBank and the Office of Finance relies heavily on information systems and other technology to conduct and manage business. Over the years, information security threats to the financial services industry have become increasingly sophisticated and could pose a significant risk to the FHLBank System. Information security incidents can potentially compromise sensitive, confidential, and personally identifiable information, and disrupt FHLBank System operations. Security incidents can affect the integrity and availability of business-critical information and systems and expose an institution to reputational risks and potential financial risks.

Information Security and Cybersecurity Risk

Information security is the process by which an organization protects the creation, collection, storage, use, transmission, and disposal of information, including the protection of hardware and infrastructure used to store and transmit such information. The commonly accepted objectives for information security include the confidentiality, integrity, and availability of information and systems, which are essential to the overall safety and soundness of an organization.

While information security describes the overall protection of information systems, the term cybersecurity[1] is more narrowly focused on the protection of digital information by preventing, detecting, and responding to attacks against information systems and their content. Consequently, cybersecurity may be viewed as a sub-discipline of information security.

Supervisory Expectations for the FHLBank's and the Office of Finance's Information Security and Cybersecurity Risk Management

FHFA's Prudential Management and Operations Standards (PMOS) require that the FHLBanks and the Office of Finance have secure information systems.[2] FHFA has communicated its

[1] Cybersecurity risk includes intentional and unintentional acts that may jeopardize the confidentiality, integrity, or availability of information technology assets and data under control. Cybersecurity risk can take the form of a variety of circumstances to cause harm to entities, their service providers, and the economy in general. These circumstances include, but are not limited to, supply chain risks such as suppliers not meeting cybersecurity requirements; social engineering such as phishing; or malicious activity such as denial-of-service attacks and viruses.

[2] *See* PMOS, 12 C.F.R. Part 1236, Appendix to Part 1236. In AB 2017-02 FHFA identifies three relevant PMOS that articulate guidelines for the board and management when establishing internal controls and information systems (Standard 1); overall risk management processes (Standard 8); and maintenance of adequate records (Standard 10).

supervisory expectations for the FHLBank's and the Office of Finance's information security and cybersecurity risk management through the following advisory bulletins (AB):

- AB 2014-02, *Operational Risk Management*, describes the four basic program components to manage operational risk effectively – risk identification and assessment, measurement and modeling, reporting, and risk management decision-making.

- AB 2016-04, *Data Management and Usage*, communicates supervisory expectations for the management of data including expectations for data governance, architecture, quality, and security.

- *AB 2017-02, Information Security Management*, provided guidance to the FHLBank System on how to approach information security management in a way that supports a safe and sound operational environment and promotes the resilience of that FHLBank System. This guidance includes principles that align with the National Institute of Standards and Technology's (NIST), Cybersecurity Framework objectives: Govern, Identify, Protect, Detect, Respond, and Recover.[3]

- AB 2018-04, *Cloud Computing Risk Management*, provides guidance to the regulated entities on assessing and managing risks associated with third-party cloud providers.

- AB 2018-08, *Oversight of Third-Party Provider Relationships*, provides guidance on assessing and managing risks associated with third-party provider relationships including information security risks.

- AB 2019-01, *Business Resiliency Management*, refers to the regulated entity's ability to minimize the impact of disruptions such as those caused by cybersecurity incidents and maintain business operations at predefined levels.

- *AB 2023-02, Supplemental Guidance to Advisory Bulletin 2017-02 - Information Security Management*, elaborated and clarified elements of AB 2017-02 on topics such

[3] NIST, a non-regulatory federal agency within the United States Department of Commerce, is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems which also can be applied to nongovernmental organizations. NIST also developed guidance to help industry, government agencies, and other organizations to manage cybersecurity risks. This guidance includes six main objectives to manage and reduce cybersecurity risks: (1) *Govern* - the organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored, (2) *Identify* – the organization's current cybersecurity risks are understood, (3) *Protect* – safeguards to manage the organization's cybersecurity risks are used, (4) *Detect* – possible cybersecurity attacks and compromises are found and analyzed, (5) *Respond* – actions regarding a detected cybersecurity incident are taken, and (6) *Recover* – assets and operations affected by a cybersecurity incident are restored.

as resiliency against cyberattacks, how to manage current information security threats, and threats from third-party providers.

AB 2017-02 and AB 2023-02 encourage the FHLBank System to align respective information security programs with appropriate industry standards, such as those promulgated by NIST commensurate with the complexity and risk profile of the entity.

Annual Examinations of the FHLBanks and the Office of Finance

DBR conducts risk-based supervisory activities pertaining to the FHLBanks, including annual examinations, periodic visitations, special reviews, and offsite monitoring of each FHLBank.[4] DBR relies on these supervisory activities to reach conclusions on each FHLBank's overall condition and the adequacy of its risk management practices. At the conclusion of an examination, DBR issues a report of examination to each FHLBank's board of directors. The report of examination communicates substantive examination conclusions, principal findings, including all MRAs,[5] and the composite and component CAMELSO ratings.[6]

DBR Guidance for Oversight of the FHLBank's and the Office of Finance's Information Security and Cybersecurity Risk Management

The Information Security Management module and workprogram provide examiners with guidance and suggested worksteps to conduct examinations of the FHLBank's and Office of Finance's information security and cybersecurity risk management.[7]

---

[4] Beginning in the 2026 supervisory cycle, DBR transitioned to a continuous supervision program that consists of targeted examinations and ongoing monitoring of the FHLBank System.

[5] AB 2017-01, *Classifications of Adverse Examination Findings*, identifies three broad classifications of findings: MRAs, which are the most serious; recommendations; and violations. MRAs consist of either "critical supervisory matters (the highest priority), which pose substantial risk to the safety and soundness of the regulated entity" or "deficiencies," which if not corrected, could "escalate and potentially negatively affect" the regulated entity. 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. Violations are matters in which an examination discloses noncompliance with laws, regulations, or orders.

[6] CAMELSO is a risk-focused rating system under which each FHLBank is assigned a composite rating based on an evaluation of various aspects of its operations. The components evaluated are Capital, Asset Quality, Management, Earnings, Liquidity, Sensitivity to Market Risk, and Operational Risk.

[7] FHFA, *FHFA Examination Manual*, Information Security module and workprogram was issued as a supplemental "field test" module in March 2017. It was finalized and replaced by the Information Security Management module and workprogram in July 2025. The July 2025 version contains mostly the same basic requirements as the field test version.

Examiners conduct and document their work in accordance with DBR's Operating Procedure Bulletins (OPBs), which are as follows:

- 2012-DBR-OPB-03, *Work Program Minimum Frequency Guidelines,* establishes minimum frequency guidelines for completing the work programs for DBR's supervision staff use in an examination's onsite scope. The Information Security Management workprogram has been assigned an annual minimum frequency.
- 2016-DBR-OPB-01, *Federal Home Loan Bank Examination Workpaper Standards,* establishes expectations for the standards and quality of examination workpapers.
- 2017-DBR-OPB-01, *Federal Home Loan Bank Adverse Examination Findings Processes,* describes MRAs along with the controls DBR implements to ensure adverse findings are remediated.
- 2018-DBR-OPB-03, *Quality Control Program*, sets forth DBR's guidance for implementing its quality control program for examination workpapers. The primary responsibility for quality control rests with DBR staff, supervisors, and executives directly involved in preparing and reviewing work products. As an additional assurance of quality, DBR's Quality Control Branch (QCB) performs reviews of selected DBR work products.

OBJECTIVE AND SCOPE

The objective of our audit was to determine whether DBR provided sufficient oversight of the FHLBank System's information security and cybersecurity risk management. The audit scope included DBR's examinations of the FHLBank's and the Office of Finance's management of information security and cybersecurity from October 1, 2024, through September 30, 2025 (audit scope).

For details on methodology see Appendix I.

RESULTS

We determined that DBR provided sufficient oversight of the FHLBank System's information security and cybersecurity risk management and generally complied with its guidance for conducting examination activities. Specifically, we concluded the following:

- DBR's Information Security Management module and workprogram provides examiners with the worksteps needed to review and evaluate the FHLBank System's information security and cybersecurity risk management practices consistent with supervisory expectations detailed in FHFA's ABs.

- DBR performed examination activities over information security and cybersecurity risk management for 10 FHLBanks and the Office of Finance in accordance with the annual minimum frequency requirement.[8]

- DBR provided risk-based coverage of the FHLBank and the Office of Finance in our sample of four examinations. This comprised performing 32 individual Information Security Management workprogram worksteps which assessed risk management practices for aspects of all six NIST control objectives.[9] Additionally, the risk-based coverage included DBR's assessment of the design of vulnerability scans and penetration testing.

- DBR's examiners documented independent analyses for 31 of 32 individual Information Security Management workprogram worksteps (96.9 percent) to support supervisory conclusions across the four examinations in our sample, as required by DBR's workpaper standards. However, an examiner did not document independent analysis of one workstep assessing the design of an FHLBank's vulnerability scans and penetration testing that supported the conclusion that the FHLBank maintains a satisfactory vulnerability management program. Furthermore, DBR's quality control program did not detect and correct this omission (see Finding). While the independent analysis was not documented, we noted that some vulnerability management reports in the examination file and certain work related to vulnerabilities in the Third-Party Risk Management workprogram supported supervisory conclusions on vulnerability management.

- DBR effectively monitored the progress of corrective actions as outlined in each FHLBanks' and Office of Finance's remediation plan for the 14 open information

[8] During our audit scope, DBR completed 12 Information Security Management workprograms which included 10 FHLBanks (the workprogram was performed twice at one FHLBank and not performed at one FHLBank) and the Office of Finance.

[9] See footnote 3 for NIST objectives.

security and cybersecurity-related MRAs. DBR also assessed the FHLBanks' remediation of the eight information security and cybersecurity-related MRAs closed during our audit scope in accordance with DBR's adverse examination findings guidance, concluding that the corrective actions were satisfactorily resolved.

Overall, we found that DBR examiners were qualified and experienced to perform the Information Security Management workprogram examinations. However, as described in the finding below, we noted that DBR's quality control program did not detect and correct a documentation deficiency to sufficiently support an examiner's supervisory conclusion.

Finding: A Documentation Deficiency was Not Detected by DBR's Quality Control Program

DBR's quality control program did not detect and correct an instance in which the examiner analysis supporting a supervisory conclusion was not documented. Specifically, an examiner did not document an independent analysis for 1 of the 32 Information Security Management workprogram worksteps (3.1 percent) to support the conclusion on a FHLBank's vulnerability management program as required by DBR's workpaper standards.[10] Furthermore, supervisory and independent reviews by DBR's QCB did not catch the omission.

According to 2018-DBR-OPB-03, *Quality Control Program*, "Supervisors should review work products for staff members as necessary for quality control and other purposes to assure appropriate support and adherence to standards." Further the OPB states "Project Team Leads ... are responsible for ensuring that … documentation adequately evidences the work performed and agrees with conclusions in written work products," but notes that the Project Team Leads may rely on other reviewers, for example, QCB staff, to meet this responsibility. A QCB Sectional Review, "assesses the workpapers of a specific examination activity, i.e., typically associated with an examination work program area. The review is a comprehensive assessment of summary memorandum and supporting documentation in the section."

The examiner, who omitted an independent analysis of vulnerability management workstep, reported meeting with the FHLBank management to discuss the institution's vulnerability management program. According to the examiner, the program had not changed significantly from the prior year, and a review of vulnerability statistics revealed no concerns. The examiner explained that, given the program's low risk profile, the minimal changes from the previous year, and competing priorities involving higher-risk areas, the analysis was not documented. DBR officials conceded that the quality control program should have detected and required correction of the documentation issue. Vulnerability management work was documented in other parts of

[10] According to the DBR Workpaper Standards OPB, "Workpapers need to provide evidence that the examiner performed independent analysis that clearly supports examination findings, conclusions, and ratings."

the Information Security Management workprogram and the Third-Party Risk Management workprogram.

Complete examination documentation is critical in demonstrating that examiners performed independent analysis to clearly support examination conclusions. The risk of incorrect supervisory conclusions increases when DBR's quality control program does not detect and correct examination workpaper deficiencies.

Recommendation

We recommend that the DBR Deputy Director:

1. Reinforce, through training and other periodic reminders to supervisory examiners and QCB staff, the requirement that all worksteps supporting supervisory conclusions must be fully completed and all analyses thoroughly documented.

FHFA COMMENTS AND OIG EVALUATION.....

We provided FHFA management an opportunity to review and provide technical comments on a draft of this audit report. We considered those comments in finalizing this report. In a written response, management agreed with our recommendation and stated that DBR will provide training to its examiners and QCB staff by August 31, 2026, to reinforce that examination worksteps must be fully completed and all analysis thoroughly documented. DBR will also provide periodic reminders in the future, as necessary.

We consider FHFA's planned corrective actions responsive to the recommendation in this report. FHFA's written response, in its entirety, is included as Appendix II in this report.

APPENDIX I: METHODOLOGY

To accomplish our objective, we performed the following procedures:

- Reviewed Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* (GAO-14-704G; September 2014), applicable during the audit scope,[11] and determined that the control activities component of internal control was significant to this objective. We focused on the underlying principles that management should: (1) design control activities to achieve objectives and respond to risks; (2) implement control activities through policies; and (3) establish expectations of competence for key roles, and other roles at management's discretion, to help the entity achieve its objectives.
- Reviewed the following laws, regulations, and guidelines significant within the context of the audit objective:
  - Cybersecurity Information Sharing Act of 2015
  - Gramm-Leach-Bliley Act
  - 12 C.F.R. Part 1235, Record Retention For Regulated Entities and Office of Finance
  - 12 C.F.R. Part 1236 and Appendix to 12 C.F.R. Part 1236 – Prudential Management and Operations Standards
- Reviewed the following FHFA supervisory guidance to identify FHFA's supervisory expectations related to the FHLBank's and Office of Finance's implementation of PMOS on management of information security and cybersecurity risks.
  - AB 2023-02, *Supplemental Guidance to Advisory Bulletin 2017-02 - Information Security Management* (January 2023)
  - AB 2019-01, *Business Resiliency Management* (May 2019)
  - AB 2018-08, *Oversight of Third-Party Provider Relationships* (September 2018)

[11] GAO, *Standards for Internal Control in the Federal Government* (GAO-14-704G) issued in September 2014 was applicable during our audit scope. The 2014 version has been superseded by GAO's *Standards for Internal Control in the Federal Government* (GAO-25-107721) which was issued in May 2025 and is effective beginning in fiscal year 2026.

- AB 2018-04, *Cloud Computing Risk Management* (August 2018)
- AB 2017-02, *Information Security Management* (September 2017)
- AB 2016-04, *Data Management and Usage* (September 2016)
- AB 2014-02, *Operational Risk Management* (February 2014)

- Reviewed the following FHFA examination modules and workprograms to identify examination guidance and suggested worksteps for examiners to conduct examinations of the FHLBank's management information security and cybersecurity risks:
  - FHFA Examination Manual, Information Security module and workprogram (Field Test version March 2017, updated to Information Security Management July 2025)
  - FHFA Examination Manual, Information Technology Risk Management Program module and workprogram (January 2017, updated May 2025)
- Reviewed the following DBR guidance to identify requirements for DBR's supervisory activities:
  - 2012-DBR-OPB-03**,** *Work Program Minimum Frequency Guidelines* (updated June 5, 2024)
  - 2016-DBR-OPB-01, *Federal Home Loan Bank Examination Workpaper Standards* (updated September 9, 2020)
  - 2017-DBR-OPB-01**,** *Federal Home Loan Bank Adverse Examination Findings Processes* (updated January 31, 2022)
  - 2018-DBR-OPB-03, *Quality Control Program* (updated December 21, 2021)
- Reviewed the following cybersecurity guidance and best practices to gain an understanding of the current information security and cybersecurity risk management objectives and internal controls:
  - The National Institute of Standards and Technology, *Cybersecurity Framework* (February 2024)
  - Cybersecurity and Infrastructure Security Agency, *Cross-Sector Cybersecurity Performance Goals* (March 2023)
  - Center for Internet Security, *CIS Critical Security Controls* (March 2025)

- Federal Financial Institutions Examination Council, *Information Security Booklet* (September 2016)

- Reviewed prior OIG reports to identify findings and recommendations related to the FHLBanks' information security and cybersecurity risk management and determined there was no impact on our audit.
  - FHFA-OIG, *Compliance Review of DBR's Assessment and Documentation of Critical Cybersecurity Controls in Examinations of the FHLBank System* (June 15, 2021) (COM-2021-005)
  - FHFA-OIG, *FHFA Should Enhance Supervision of its Regulated Entities' Cybersecurity Risk Management by Obtaining Consistent Cybersecurity Incident Data* (Sept. 23, 2019) (EVL-2019-004)
  - FHFA-OIG, *Compliance Review of DBR's Examinations of Critical Cybersecurity Controls at the Federal Home Loan Banks* (May 7, 2019) (COM-2019-004)
  - FHFA-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)

- Interviewed DBR examination team personnel to gain an understanding of the DBR's oversight of the FHLBank System's information security and cybersecurity risk management. DBR examination team personnel included Associate Director, Supervisory Examiner, and Senior Management Analyst. Obtained written responses, as needed, from DBR personnel to address questions and observations related to our audit testing procedures.

- Compared DBR's FHFA Examination Manual and DBR's Information Security Management module and workprogram to FHFA's PMOS, FHFA's Advisory Bulletins, and external information security standards and best practices, to determine whether DBR's examination guidance (1) is consistent with FHFA's criteria and/or supervisory expectations for information security and cybersecurity risk management; (2) is consistent with control objectives of risk management practices derived from external information security standards and best practices; and (3) provides examiners the necessary worksteps to review and evaluate the FHLBank System's information security and cybersecurity risk management practices.

- Identified the 12 Information Security Management workprograms completed during the audit scope (workprogram was performed twice at one FHLBank, once at nine

FHLBanks and the Office of Finance, and not performed at one FHLBank), confirmed the population of workprograms with DBR, and assessed whether the workprograms were performed in accordance with the annual minimum frequency requirement. For the one FHLBank where the Information Security Management workprogram was not performed, we confirmed whether DBR completed the workprogram in the months prior to and after our audit scope.

- Selected a non-statistical, risk-based sample of 4 of the 12 examinations in our population (33 percent) based on our (1) review of DBR reports of examination to identify MRAs related to information security and cybersecurity; (2) discussion with DBR and OIG investigators for relative information security and cybersecurity risk at each of the FHLBanks and the Office of Finance; (3) review of a list of cybersecurity incidents the FHLBanks and the Office of Finance reported to DBR from October 1, 2023, through September 30, 2025.

- Reviewed the pre-examination analysis memoranda, workprograms and supporting documentation, and activity memoranda for Information Security Management workprogram completed at each selected FHLBanks and the Office of Finance during the audit scope period to determine whether:

    - The pre-examination analysis memorandum documents the agreed-upon approach (objectives, scope, and worksteps) for the examination and is consistent with the Supervisory Strategy.

    - All changes in scope were documented and approved by the EIC and Associate Director.

    - The worksteps documented in the workprogram were consistent with the pre-examination analysis memorandum and conclusions are supported by independent, examiner analysis.

    - Conclusions in the analysis memoranda logically flow from the workprogram and adverse conclusions resulted in the appropriate type of adverse examination finding.

- Compared DBR's overall examination coverage in the selected examinations to the information security and cybersecurity risk areas detailed in FHFA's ABs, aligned with NIST's Cybersecurity Framework objectives, to determine whether DBR examinations provide risk-based coverage of the FHLBank's information security and cybersecurity risk management.

- Reviewed the examiner's assessment of the design of vulnerability scans and penetration testing performed in the selected examinations and determined whether the examiner

documented that the (1) parties that perform the vulnerability scans and penetration test are sufficiently independent; (2) institution's security risk assessment informs the frequency of the vulnerability and penetration tests; (3) scopes and strategies of the vulnerability scans and penetration tests are commensurate with the institution's technology environment; and (4) institution adequately addressed the findings from such vulnerability scans and penetration tests or has an adequate plan for remediation.

- Determined, based on our review of Information Security Management workprograms completed during the scope period and confirmation with DBR, the population of 11 examiners responsible for completing these workprograms. We assessed the qualifications and experience for 9 of these examiners against DBR's established expectations of competence (i.e., position description for a specialized information technology examiner role) to determine whether the examination staff members who conduct and supervise the Information Security Management workprogram for each FHLBank and the Office of Finance, taken as a whole, have the qualifications and experience to effectively perform the work. Two of the 11 examiners had retired before we began our audit fieldwork, and since documentation of detailed qualifications and experience was not available for these two examiners, we made general inquiries about their qualifications.

- Assessed DBR's monitoring of corrective actions for the 14 open MRAs related to information security and cybersecurity to determine the effectiveness of supervisory follow-up. For the eight of these MRAs closed during the audit scope, we assessed whether DBR ensured their remediation in accordance with 2017-DBR-OPB-01, *FHLBank Adverse Examination Findings Processes*.

We conducted this performance audit from October 2025 to May 2026 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 II: FHFA MANAGEMENT RESPONSE.....

This page intentionally blank. See the following page.

Federal Housing Finance Agency

MEMORANDUM

TO: James Hodge, Deputy Inspector General for Audits

FROM: Joshua Stallings, Deputy Director, Division of FHLBank Regulation

JOSHUA STALLINGS Digitally signed by JOSHUA STALLINGS Date: 2026.05.04 10:54:56 -04'00'

SUBJECT: Audit Report: *DBR's Quality Control Program Did Not Detect a Documentation Deficiency in Its Oversight of the FHLBank System's Information Security and Cybersecurity Risk Management*

DATE: May 1, 2026

Thank you for the opportunity to respond to the Office of Inspector General's (OIG) draft report. The objective of OIG's audit was to assess whether the Division of FHLBank Regulation (DBR) provided sufficient oversight of the FHLBank System's information security and cybersecurity risk management.

While the report identified that DBR provided sufficient oversight, it included a finding and recommendation related to DBR's quality control program not detecting and correcting an instance in which the examiner analysis supporting a supervisory conclusion was not documented in the examination workpapers. The Agency agrees with the recommendation.

Recommendation 1:
We recommend that the DBR Deputy Director:

1. *Reinforce, through training and other periodic reminders to supervisory examiners and QCB staff, the requirement that all worksteps supporting supervisory conclusions must be fully completed and all analyses thoroughly documented.*

Management Response: FHFA agrees to take action in response to the recommendation. By August 31, 2026, DBR will provide training to its examiners and Quality Control Branch (QCB) to reinforce that examination work steps must be fully completed and all analysis thoroughly documented. DBR will also provide periodic reminders in the future as necessary.

If you have any questions related to this response, please contact Ed Stolle.

cc: Ivan Bengtson
Ed Stolle

Federal Housing Finance Agency
Office of Inspector General

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