Federal Housing Finance Agency
Office of Inspector General

Compendium of Open Recommendations

November 1, 2026

TABLE OF CONTENTS .....

ABBREVIATIONS 3
INTRODUCTION 4
Tracking of OIG Recommendations 4
Validation Testing 4
OPEN RECOMMENDATIONS 6
CLOSED RECOMMENDATION 23

ABBREVIATIONS .....

DER	Division of Enterprise Regulation
Enterprises	Fannie Mae and Freddie Mac
FHFA	Federal Housing Finance Agency
OIG	Federal Housing Finance Agency Office of Inspector General
ROE	Report of Examination

INTRODUCTION

Since the Federal Housing Finance Agency (FHFA) Office of Inspector General (OIG) began operations in October 2010, we have made more than 775 recommendations to FHFA.[1] Our recommendations are targeted to improve efficiency and effectiveness and to reduce fraud, waste, and abuse at FHFA and the entities it oversees.

To maintain the focus on opportunities for improvement that our recommendations identify, every month, we publish an updated version of this report on our website, setting forth all open recommendations from our audits, evaluations, and other studies.[2] For additional information on any recommendation, please click on the hyperlinked report title to access its underlying report.[3] This compendium is comprehensive as of November 1, 2026.

Tracking of OIG Recommendations

Our recommendations, like those of other inspectors general, are primarily made in reports issued by our Offices of Audits and Evaluations. We report the facts, as found, and recommend actions to address any shortcomings we identify. We provide FHFA the opportunity to respond in writing to our recommendations. FHFA's determinations on whether to agree with our recommendations are included in our published reports.

Once FHFA completes a corrective action, we review the action and, if it comports with our recommendation, we close the recommendation. Should the Agency reject a recommendation, or decline to implement an acceptable corrective action, then we close the recommendation as rejected. In either case, we include any new closures of recommendations in this compendium.

Validation Testing

We rely on materials and representations from the Agency to close recommendations. Accordingly, we are not always able to assess, at the time of closure, whether the implementation actions by FHFA meet the letter and spirit of the agreed-upon recommendation, nor can we determine, at closure, the longer-term impact of the

[1] Includes public and non-public recommendations.

[2] This report does not include recommendations under consideration for work that is in progress.

[3] Each recommendation in this report is listed by report number followed by the specific recommendation number. For example, AUD-2025-007-1 denotes this is the first recommendation in report AUD-2025-007.

recommendation. As needed, we conduct validation testing of closed recommendations. This testing enhances accountability and adds value to FHFA and the American taxpayers it serves.

Together with its other responsibilities, the Office of Evaluations examines selected closed recommendations to assess independently FHFA's implementation of the corrective actions it represented to us that it intended to take, as well as the impact of those actions, and publishes reports of its validation testing in "compliance reviews." These compliance reviews enable our stakeholders to assess the impact of our recommendations, as well as the efficacy of the Agency's implementation of those recommendations.

Any open recommendations contained in published compliance reviews are included in this compendium.

OPEN RECOMMENDATIONS .....

Open Recommendation	Report Title and Date
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	Audit of the Federal Housing Finance Agency's Information Security Program Fiscal Year 2020 (AUD-2021-001-3, October 20, 2020)
FHFA should assess whether the Office of Technology and Information Management has sufficient, qualified staff to complete required updates and testing of its contingency plans in accordance with FHFA's standard and National Institute of Standards and Technology requirements, and address any resource constraints that have adversely affected the Office of Technology and Information Management's ability to carry out its contingency planning requirements.	FHFA Did Not Follow All of its Contingency Planning Requirements for the National Mortgage Database (NMDB) or its Correspondence Tracking System (CTS) (AUD-2022-003-3, December 13, 2021)
The FHFA Office of General Counsel's Designated Agency Ethics Official or Alternate Designated Agency Ethics Official should improve the Agency's existing internal controls over its employee financial disclosure process by performing and documenting technical reviews and conflict of interest analysis within 60 days of receiving employee financial disclosure reports as required by Office of Government Ethics regulations and FHFA policy.	FHFA Did Not Always Follow Federal Regulations and Its Policy for Employee Financial Disclosures During Fiscal Years 2020 and 2021 (AUD-2022-011-1, September 8, 2022)
The FHFA Office of General Counsel's Designated Agency Ethics Official or Alternate Designated Agency Ethics Official should improve FHFA's existing internal controls over its employee financial disclosure process by ensuring that employees file their financial disclosure reports timely as required by Office of Government Ethics regulations and FHFA policy.	FHFA Did Not Always Follow Federal Regulations and Its Policy for Employee Financial Disclosures During Fiscal Years 2020 and 2021 (AUD-2022-011-3, September 8, 2022)

Open Recommendation	Report Title and Date
FHFA's Chief Information Officer should develop and maintain a complete and accurate cloud system component inventory, as required by National Institute of Standards and Technology Special Publication 800-53.	FHFA Did Not Fully Implement Select Security Controls Over One of Its Cloud Systems as Required by NIST and FHFA Standards and Guidelines (AUD-2023-002-2, March 8, 2023)
FHFA's Chief Information Officer should develop and implement a solution to encrypt all data-at-rest on the cloud system as required by National Institute of Standards and Technology Special Publication 800-53.	FHFA Did Not Fully Implement Select Security Controls Over One of Its Cloud Systems as Required by NIST and FHFA Standards and Guidelines (AUD-2023-002-5, March 8, 2023)
FHFA should develop, document, and implement control activities to ensure that (a) only current FHFA employees are receiving transportation benefits, (b) no employee is improperly participating in both transportation benefit programs, (c) the Transit Benefits System has a record/certification for each employee who receives a transportation benefit, and (d) SmarTrip® cards are physically controlled. Such control activities include periodic reconciliation of approved transit subsidy recipients in the Transit Benefits System to FHFA transit subsidy recipients listed on the Washington Metropolitan Area Transit Authority Monthly Activity Reports, periodic reconciliation of approved transit subsidy recipients to active parking permit recipients, and periodic inventory counts of SmarTrip® cards registered to FHFA and undistributed parking permits. [Closed in June 2019; reopened upon results of compliance testing.]	FHFA Needs to Strengthen Controls over its Employee Transportation Benefits Programs (AUD-2018-013-1, September 25, 2018) and FHFA Did Not Effectively Implement Controls Intended to Ensure the Integrity of Its Employee Transportation Benefits Program (COM-2023-005, June 21, 2023)[4]

[4] When we reopen a recommendation, we typically will not issue a new recommendation number.

Open Recommendation	Report Title and Date
FHFA should ensure that the Transit Benefits System has accurate and up-to-date records of, and current certifications for, each FHFA employee who receives a transportation benefit. [Closed in June 2019; reopened upon results of compliance testing.]	FHFA Needs to Strengthen Controls over its Employee Transportation Benefits Programs (AUD-2018-013-2, September 25, 2018) and FHFA Did Not Effectively Implement Controls Intended to Ensure the Integrity of Its Employee Transportation Benefits Program (COM-2023-005, June 21, 2023)
FHFA's Acting Chief Information Officer should remediate past due exploitable vulnerabilities in accordance with Cybersecurity and Infrastructure Security Agency Binding Operating Directive 22-01 and the Office of Technology and Information Management Vulnerability Management Process.	Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2023 (AUD-2023-004-3, July 26, 2023)
FHFA's Chief Information Officer should restrict user access to the folders and files on FHFA's network in accordance with least privilege principle.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2024-007-1, August 12, 2024)
FHFA's Chief Information Officer should identify and implement a solution, in coordination with vendors, to ensure that multifactor authentication is required to access FHFA's network. If there are no viable solutions, document any risk-based decisions, including compensating controls.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2024-007-7, August 12, 2024)
FHFA's Chief Information Officer should identify and implement a solution to detect and monitor the transfer of large amounts of data moving across FHFA's network.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2024-007-11, August 12, 2024)

Open Recommendation	Report Title and Date
FHFA's Chief Information Officer should identify and implement a solution to detect and prevent controlled unclassified information or personally identifiable information from being transferred outside of FHFA's network to personal accounts on email and cloud-based storage services.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2024-007-12, August 12, 2024)
FHFA's Chief Information Officer should determine whether resources can be made available to implement a data loss prevention system to prevent the exfiltration of controlled unclassified information.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2024-007-13, August 12, 2024)
FHFA's Chief Information Officer should reevaluate the former Acting Chief Information Officer's risk acceptance related to portable software programs, and implement security controls to detect and prevent users from downloading and running unapproved software on FHFA's system in accordance with National Institute of Standards and Technology and FHFA's Rules of Behavior.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2024-007-14, August 12, 2024)
FHFA's Chief Information Officer should monitor and respond to unauthorized software downloads in accordance with FHFA's Common Control Plan.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2024-007-15, August 12, 2024)
FHFA's Chief Information Officer should develop a Plan of Action and Milestones to track the remediation of past due Cybersecurity and Infrastructure Security Agency Known Exploitable Vulnerabilities in accordance with Cybersecurity and Infrastructure Security Agency's Binding Operational Directive 22-01 and FHFA's Office of Technology and Information Management Vulnerability Management Process, Revision 2.7 (September 7, 2022). FHFA's Office of Technology and Information Management should implement compensating controls (i.e., isolating systems with un-remediated vulnerabilities) to mitigate the risk of the vulnerabilities.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2024-007-17, August 12, 2024)

Open Recommendation	Report Title and Date
FHFA's Chief Information Officer should prioritize existing Office of Technology and Information Management resources based on the Plan of Action and Milestones to ensure that Cybersecurity and Infrastructure Security Agency Known Exploitable Vulnerabilities are remediated in accordance with Cybersecurity and Infrastructure Security Agency's Binding Operational Directive 22-01 and FHFA's Office of Technology and Information Management Vulnerability Management Process, Revision 2.7 (September 7, 2022).	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2024-007-18, August 12, 2024)
FHFA's Chief Information Officer should implement security controls to lock down Universal Serial Bus ports so that only authorized Universal Serial Bus devices are allowed.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2024-007-21, August 12, 2024)
FHFA's Chief Information Officer should perform annual testing of the contingency plan in accordance with the recovery procedures document to ensure failover and failback are conducted as planned.	FHFA's Disaster Recovery Exercise for Its General Support System Needs Improvement (AUD-2024-010-4, September 25, 2024)
FHFA's Chief Information Officer should encrypt all backup data-at-rest at FHFA's alternate site and update the existing Plan of Action and Milestones to include compensating controls until the Plan of Action and Milestones has been closed.	FHFA's Disaster Recovery Exercise for Its General Support System Needs Improvement (AUD-2024-010-6, September 25, 2024)
FHFA's Division of Enterprise Regulation (DER) should consider whether to direct Freddie Mac to file an amended Suspicious Activity Report containing a complete narrative for the case identified above, and whether to amend FHFA's examination procedures to require this step if future examinations uncover a similar issue.	Inspection: FHFA Oversight of Freddie Mac's Issuance of Suspicious Activity Reports (COM-2025-005-2, March 27, 2025)

Open Recommendation	Report Title and Date
FHFA's Office of Facilities and Operations Management Associate Director, in coordination with the Office of Human Resources Management should finalize and implement policies and procedures for the Agency's administration of the background investigations and adjudication processes for federal and contractor employees that (a) are consistent with regulations and implementation guidance issued by the United States Office of Personnel Management; (b) assigns roles and responsibilities; (c) establishes specific procedures; and (d) measures operational effectiveness criteria.	FHFA's Controls Over Background Investigations and Adjudications Were Ineffective (AUD-2025-002-1, March 28, 2025)
FHFA's Chief Information Officer should establish and implement guidance for performing National Institute of Standards and Technology Cybersecurity Framework 2.0 activities through policies and procedures.	Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2025 (AUD-2025-004-1, July 30, 2025)
FHFA's Chief Information Officer should create a Plan of Action and Milestones to establish when the annual Disaster Recovery Procedures for FHFA Production Systems exercise will be conducted and when the new system owners will be assigned and trained on their roles and responsibilities related to FHFA General Support System, Office of General Counsel Matter Management Tracking System, and the FHFA Status Tracking and Reporting system.	Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2025 (AUD-2025-004-5, July 30, 2025)
FHFA's Chief Information Officer should schedule and conduct an annual Disaster Recovery Procedures for FHFA Production Systems exercise for the FHFA General Support System, Office of General Counsel Matter Management Tracking System, and the FHFA Status Tracking and Reporting system, and ensure new system owners are trained to execute them.	Audit of the Federal Housing Finance Agency's Information Security Programs and Practices Fiscal Year 2025 (AUD-2025-004-6, July 30, 2025)

Open Recommendation	Report Title and Date
FHFA's Division of Federal Home Loan Bank Regulation should assess the extent to which Federal Home Loan Banks are relying on redacted ROEs (reports of examination) when reviewing membership applications or performing ongoing monitoring.	FHFA and FHLBank Coordination with Regulators Improved After the Spring 2023 Bank Failures, but Several FHLBanks Faced Challenges Obtaining Timely Supervisory Information (EVL-2025-005-1, September 18, 2025)
FHFA's Division of Federal Home Loan Bank Regulation should clarify and reinforce Division of Federal Home Loan Bank Regulation's expectation to the Federal Home Loan Banks that they should request and receive from federal and state regulators ROEs that are not substantively redacted, and that other relevant supervisory reports should be collected when necessary.	FHFA and FHLBank Coordination with Regulators Improved After the Spring 2023 Bank Failures, but Several FHLBanks Faced Challenges Obtaining Timely Supervisory Information (EVL-2025-005-2, September 18, 2025)
FHFA's Division of Federal Home Loan Bank Regulation should conduct outreach to federal financial regulators to reinforce the need for compliance with 12 U.S.C. § 1442(a)(1), which requires their production of reports, records, and information relating to the condition of any member of any Federal Home Loan Bank upon request by a Federal Home Loan Bank. As part of this outreach, make clear that such materials extend beyond ROEs, and that materials produced in response to a Federal Home Loan Bank requests should be provided without substantive redactions.	FHFA and FHLBank Coordination with Regulators Improved After the Spring 2023 Bank Failures, but Several FHLBanks Faced Challenges Obtaining Timely Supervisory Information (EVL-2025-005-3, September 18, 2025)
FHFA's Division of Federal Home Loan Bank Regulation should assess the extent to which restrictions on access to state-issued ROEs may hinder the Federal Home Loan Banks in making fully informed decisions when evaluating applications for membership and when making determinations to limit or deny member requests for advances in accordance with applicable FHFA regulations.	FHFA and FHLBank Coordination with Regulators Improved After the Spring 2023 Bank Failures, but Several FHLBanks Faced Challenges Obtaining Timely Supervisory Information (EVL-2025-005-4, September 18, 2025)

Open Recommendation	Report Title and Date
FHFA's Division of Federal Home Loan Bank Regulation should, if applicable, continue to pursue outreach with the Conference of State Bank Supervisors and state regulators to assist Federal Home Loan Banks in accessing state-issued ROEs.	FHFA and FHLBank Coordination with Regulators Improved After the Spring 2023 Bank Failures, but Several FHLBanks Faced Challenges Obtaining Timely Supervisory Information (EVL-2025-005-5, September 18, 2025)
FHFA's Division of Federal Home Loan Bank Regulation should complete its assessment of the extent of weaknesses in the Federal Home Loan Banks' enforcement of members' material adverse change notification requirements, and provide guidance to Federal Home Loan Banks on best practices, such as issuing periodic reminders of notification requirements, to help ensure members' compliance with the Federal Home Loan Banks' contractual requirements.	FHFA and FHLBank Coordination with Regulators Improved After the Spring 2023 Bank Failures, but Several FHLBanks Faced Challenges Obtaining Timely Supervisory Information (EVL-2025-005-6, September 18, 2025)
FHFA's Chief Information Officer should restrict access to member bank submission forms and associated documents to only authenticated and authorized users.	Vulnerabilities in FHFA's Public-Facing Systems Risk Unauthorized Access to Non-Public Data (AUD-2025-007-2, September 25, 2025)
FHFA's Chief Information Officer should establish a formal content review and approval process for all documents and content posted to public-facing websites, including checks for controlled unclassified information data.	Vulnerabilities in FHFA's Public-Facing Systems Risk Unauthorized Access to Non-Public Data (AUD-2025-007-7, September 25, 2025)
FHFA's Chief Information Officer should remediate vulnerabilities by (a) applying all available software and firmware updates to the closed circuit television platform, (b) replacing or renewing expired website security certificates, and (c) conducting a secure code review to identify and remove hardcoded credentials or unsecure configurations.	Vulnerabilities in FHFA's Public-Facing Systems Risk Unauthorized Access to Non-Public Data (AUD-2025-007-19, September 25, 2025)

Open Recommendation	Report Title and Date
FHFA's Chief Financial Officer should ensure that all staff with invoice approval authority complete the updated training.	FHFA's Controls Over Legal Service Payments Were Generally Effective But Did Not Ensure Compliance With All Contractual Requirements (AUD-2026-001-4, February 17, 2026)
FHFA's Office of Human Resources Management Director should determine the allowability of the questioned reimbursement and stipend costs totaling $65,690 and take appropriate action including recoupment of funds.	FHFA Did Not Consistently Comply with Policies and Procedures for Paying Employee Reimbursements and Stipends (EVL-2026-002-1, March 30, 2026)
FHFA's Office of Human Resources Management Director should strengthen compliance with applicable policies and procedures over reimbursements and stipends through targeted training of Office of Human Resources Management staff responsible for initiating, reviewing, and approving payments. Training on the requirements of Policy 113, the Duty Station Policy, and other applicable guidance should reinforce the following: • Reimbursements must be supported by verifiable documentation of an employee's eligible job-related expenses with required, supporting documentation; • Payments must not exceed reimbursement and stipend thresholds and must be accurate; • Stipends should be issued exclusively to employees who meet eligibility criteria; and • Agreements and other certifications must be properly executed and maintained.	FHFA Did Not Consistently Comply with Policies and Procedures for Paying Employee Reimbursements and Stipends (EVL-2026-002-2, March 30, 2026)
FHFA's Office of Human Resources Management Director should develop and implement standardized controls to systematically review and verify the accuracy of out-stationed employee stipend payments for consistency across the Agency.	FHFA Did Not Consistently Comply with Policies and Procedures for Paying Employee Reimbursements and Stipends (EVL-2026-002-3, March 30, 2026)

Open Recommendation	Report Title and Date
FHFA's Office of Human Resources Management Director should conduct periodic testing of controls over reimbursements and stipends to ensure payments are made in accordance with Policy 113 and other applicable guidance.	FHFA Did Not Consistently Comply with Policies and Procedures for Paying Employee Reimbursements and Stipends (EVL-2026-002-4, March 30, 2026)
FHFA's Division of Federal Home Loan Bank Regulation Deputy Director should reinforce controls governing out-stationed employee stipends through periodic reminders and targeted training of officials responsible to ensure recipient eligibility, accurate payment through coordination with Office of Human Resources Management, as necessary, and maintenance of properly executed duty station agreements.	FHFA Did Not Consistently Comply with Policies and Procedures for Paying Employee Reimbursements and Stipends (EVL-2026-002-5, March 30, 2026)
FHFA's Division of Federal Home Loan Bank Regulation Deputy Director should train Division of Federal Home Loan Bank Regulation staff responsible for initiating, reviewing, processing, and approving stipends on the requirements of Policy 113, 2021-DBR-OPB-04, the Duty Station Policy, and any procedural updates.	FHFA Did Not Consistently Comply with Policies and Procedures for Paying Employee Reimbursements and Stipends (EVL-2026-002-6, March 30, 2026)
FHFA's Office of Human Resources Management Director should develop a centralized recordkeeping system for managing reimbursement and stipend records that allows timely and accurate retrieval of supporting documentation.	FHFA Did Not Consistently Comply with Policies and Procedures for Paying Employee Reimbursements and Stipends (EVL-2026-002-7, March 30, 2026)
FHFA's Office of Human Resources Management Director should perform periodic checks of reimbursement and stipend documents to verify that they are accurate, complete, and have been retained for the required period of time.	FHFA Did Not Consistently Comply with Policies and Procedures for Paying Employee Reimbursements and Stipends (EVL-2026-002-8, March 30, 2026)

Open Recommendation	Report Title and Date
FHFA's Office of Human Resources Management Director should provide supplemental, as-needed training to FHFA staff responsible for initiating, reviewing, and approving reimbursements and stipends on the requirements of FHFA's Records and Information Management Policy; FHFA's Comprehensive Records Schedule; and the National Archives and Records Administration's General Records Schedules when retaining information and documentation created under Policy 113 and any corresponding updates. This training should complement, not replace, other mandatory training.	FHFA Did Not Consistently Comply with Policies and Procedures for Paying Employee Reimbursements and Stipends (EVL-2026-002-9, March 30, 2026)
FHFA's Enterprise Governance, Risk, and Compliance system owner should ensure that the three privileged users are provisioned with separate standard user accounts for routine activities and use privileged accounts only when elevated access is required in accordance with National Institute of Standards and Technology Special Publication 800-53.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-1, September 28, 2026)
FHFA's Enterprise Governance, Risk, and Compliance system owner should review the 19 inactive user accounts on the Enterprise Governance, Risk, and Compliance Cloud System and determine if they should be disabled in accordance with National Institute of Standards and Technology Special Publication 800-53.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-2, September 28, 2026)
FHFA's Enterprise Governance, Risk, and Compliance system owner should in coordination with FHFA's Chief Information Officer, implement a mechanism to identify and disable user accounts after 35 days of application-level inactivity, in accordance with National Institute of Standards and Technology Special Publication 800-53.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-3, September 28, 2026)
FHFA's Enterprise Governance, Risk, and Compliance system owner should document procedures for sanitizing hotline complaint records when entering them into the system to ensure sensitive information is not included.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-4, September 28, 2026)

Open Recommendation	Report Title and Date
FHFA's Enterprise Governance, Risk, and Compliance system owner should fully sanitize the two hotline complaint records that contain sensitive information in accordance with National Institute of Standards and Technology Special Publication 800-53.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-5, September 28, 2026)
FHFA's Enterprise Governance, Risk, and Compliance system owner should remove the two hotline complaint records that were transferred to the pre-production environment in accordance with National Institute of Standards and Technology Special Publication 800-53.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-6, September 28, 2026)
FHFA's Enterprise Governance, Risk, and Compliance system owner should update the Enterprise Governance, Risk, and Compliance Cloud System Customer Controls document in accordance with National Institute of Standards and Technology Special Publication 800-18 to: a. Describe the 87 of 92 controls that FHFA was responsible for implementing for the production environment; b. Describe the security controls for the pre-production environment; c. Document all inherited controls and reference the FHFA System Security and Privacy Plan for the General Support System or FHFA Common Control Plan; d. Identify the system's name, security categorization, impact level, operational status, system type, and authorizing official; and e. Define the system's environment and security authorization boundary.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-7, September 28, 2026)
FHFA's Enterprise Governance, Risk, and Compliance system owner should reset the password of the system administrator account and ensure the new password meets the password strength requirements in accordance with the FHFA Identification and Authentication Standard.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-8, September 28, 2026)

Open Recommendation	Report Title and Date
FHFA's Enterprise Governance, Risk, and Compliance system owner should enable and enforce multifactor authentication for access to the pre-production environment in accordance with National Institute of Standards and Technology Special Publication 800-53.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-9, September 28, 2026)
FHFA's Enterprise Governance, Risk, and Compliance system owner should ensure that user accounts used for testing in the pre-production environment include information linking to the identity of the account owner in accordance with National Institute of Standards and Technology Special Publication 800-53.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-10, September 28, 2026)
FHFA's Enterprise Governance, Risk, and Compliance system owner should ensure that the contractor account includes unique identifiers in accordance with the customer responsibility matrix.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-11, September 28, 2026)
FHFA's Enterprise Governance, Risk, and Compliance system owner should ensure that audit logs for the pre-production environment are reviewed as needed or on a quarterly basis in accordance with the Enterprise Governance, Risk, and Compliance Cloud System Customer Controls document and National Institute of Standards and Technology Special Publication 800-53.	FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective (AUD-2026-006-12, September 28, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-1, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-2, September 29, 2026)

Open Recommendation	Report Title and Date
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-3, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-4, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-5, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-6, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-7, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-8, September 29, 2026)

Open Recommendation	Report Title and Date
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-10, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-11, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-12, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-13, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-14, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-15, September 29, 2026)

Open Recommendation	Report Title and Date
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-16, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-17, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-20, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-22, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-23, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-30, September 29, 2026)

Open Recommendation	Report Title and Date
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-31, September 29, 2026)
Because information in this report could be used to circumvent FHFA's internal controls, it has not been released publicly, and the recommendation text is therefore non-public.	FHFA's Security Controls Were Not Effective to Protect Its Network and Systems Against Internal Threats (AUD-2026-007-32, September 29, 2026)
FHFA's General Counsel should document procedures for the Agency's administration of the following Suspended Counterparty Program processes: (1) performing quality checks for completeness to ensure referrals are properly tracked, verified, and processed; and (2) assessing the performance of the Suspended Counterparty Program.	The Office of General Counsel Provided Sufficient Oversight of the Suspended Counterparty Program But Did Not Document Certain Controls in Its Operating Procedures (AUD-2026-009-1, September 29, 2026)
FHFA's General Counsel should ensure incorporation of the final suspension appeals process into the overall Suspended Counterparty Program Operating Procedures is completed and communicated to Suspended Counterparty Program staff.	The Office of General Counsel Provided Sufficient Oversight of the Suspended Counterparty Program But Did Not Document Certain Controls in Its Operating Procedures (AUD-2026-009-2, September 29, 2026)

CLOSED RECOMMENDATION

Set forth below is the recommendation we closed during the prior month, as well as the closure rationale.

Closed Recommendation	Closure Rationale	Report Title and Date
FHFA's Division of Federal Home Loan Bank Regulation Deputy Director should ensure that the Office of Risk Analysis and Modeling evaluates its current internal model risk management practices in line with FHFA's model risk management supervisory expectations (defined in Advisory Bulletin 2013-07 and Advisory Bulletin 2022-03) and design controls to (1) periodically review and maintain its model risk inventory (to include a risk-based validation schedule), (2) engage external resources to perform independent model validations in accordance with the validation schedule, and (3) conduct model performance tracking. Further, the Office of Risk Analysis and Modeling should update and finalize its policies and procedures to reflect the internal model risk management practices adopted.	Corrective action completed	The Division of Federal Home Loan Bank Regulation Needs to Improve Controls Over Internal Model Risk (AUD-2025-009-1, September 29, 2025)

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
- Visit: www.fhfaoig.gov/report-fraud-waste-or-abuse
- Write: FHFA Office of Inspector General
  Attn: Office of Investigations – Hotline
  400 Seventh Street SW
  Washington, DC 20219