Federal Housing Finance Agency
Office of Inspector General

FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective

Audit Report • AUD-2026-006 • September 28, 2026

EXECUTIVE SUMMARY

PURPOSE

The Enterprise Governance, Risk, and Compliance (eGRC) Cloud System is a comprehensive solution the Federal Housing Finance Agency (FHFA or Agency) uses to manage risks, ensure compliance, and support oversight activities, including tracking of hotline complaints referred by the Office of Inspector General (OIG). The system includes production and pre-production environments managed by Office of the Chief Financial Officer (OCFO) staff and contractors. Our objective for this audit was to determine whether FHFA effectively designed and implemented security controls for its eGRC Cloud System to manage access and protect information in accordance with federal standards and FHFA requirements.

RESULTS

We determined that FHFA**'s** design and implementation of select security controls for its eGRC Cloud System were not fully effective. While FHFA designed and implemented some of the security controls in accordance with federal standards and FHFA requirements, we found weaknesses in other controls. Specifically, FHFA did not consistently implement access controls for privileged and inactive accounts; did not fully document and implement data protection controls for sanitizing hotline complaints referred by the OIG; did not fully describe the controls applicable to the system in its security documentation; and did not fully implement identification and authentication controls to protect account passwords, enforce multifactor authentication, and uniquely identify users. Moreover, FHFA established audit log review procedures but did not fully implement them in the pre-production environment.

These weaknesses reduce FHFA's ability to ensure that access is appropriate, complaint information is protected, and security controls are documented. Accordingly, we are reporting five findings related to the identified weaknesses in design and implementation of controls.

RECOMMENDATIONS

We made 12 recommendations to address our findings. In a written response, FHFA management acknowledged receipt of the report but did not express agreement or disagreement with our recommendations. As such, management's response did not address our recommendations. See FHFA Comment and OIG Evaluation for more details.

This report was prepared by Zachary Lewkowicz, IT Audit Manager; Shedaun Smith, IT Specialist; Robert Todora, IT Specialist; and Raymond Harenza, IT Specialist; 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

ABBREVIATIONS

CRM	Customer Responsibility Matrix
eGRC	Enterprise Governance, Risk, and Compliance
FHFA or Agency	Federal Housing Finance Agency
FISMA	Federal Information Security Modernization Act of 2014
GAO	Government Accountability Office
GSS	General Support System
MFA	Multifactor Authentication
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Federal Housing Finance Agency Office of Inspector General
OPPR	Office of Planning, Performance, and Risk
OCFO	Office of the Chief Financial Officer
SP	Special Publication
SSPP	System Security and Privacy Plan

BACKGROUND

FHFA's Network and eGRC Cloud System

FHFA's network and systems host a variety of data and information such as financial reports and data from Fannie Mae and Freddie Mac, U.S. Financial Technology LLC (formerly known as Common Securitization Solutions, LLC), the Federal Home Loan Banks, and the Office of Finance, as well as FHFA employees' personally identifiable information. As such, it is important that the configurations and controls in place are effective to prevent unauthorized access to systems and information.

FHFA uses cloud services provided by contractors to process, store, or transmit certain FHFA mission-related information. According to the FISMA inventory conducted during fiscal year 2025, FHFA owned a total of 47 systems, 31 of which were cloud systems. FHFA's Office of Planning, Performance, and Risk (OPPR)[1] procured the services of a vendor to provide an enterprise governance, risk management, and compliance management solution to improve its capabilities. The contractor would provide licenses and resources for implementing a managed Software as a Service[2] "cloud" solution that satisfies FHFA's security, privacy, technical, and functional requirements.

On May 20, 2025, FHFA's former Chief Information Officer granted the eGRC Cloud System an authorization to operate, which was extended to October 15, 2027. The overarching purpose of the system is to track and coordinate OIG and Government Accountability Office (GAO) engagements (e.g., audits, evaluations, reviews, etc.), remediate findings, conduct assessments of FHFA internal controls, and assess and mitigate FHFA risks. The eGRC Cloud System is a comprehensive solution designed to manage risks, ensure compliance, and enhance operational resilience. The system architecture comprises multiple environments, including production[3] and

[1] FHFA's OPPR was integrated into OCFO on January 11, 2026. OCFO is responsible for the system after the integration. The Internal Control and Compliance Branch inherited responsibility for the eGRC Cloud System.

[2] Software as a Service is a delivery model where consumers are users of the provider's applications running on an underlying cloud infrastructure. Applications are accessible through various platforms. Consumers do not manage or control the underlying infrastructure. With software as a service, the consumer has the least amount of responsibility. The cloud service provider owns the security tasks for the physical infrastructure and select application-level controls. But the consumer is still responsible for security of its data and access to that data.

[3] A production environment as an operational environment in which the system performs its intended day-to-day functions and processes or provides access to production data.

pre-production,[4] and several other key components. FHFA Assistant Director of Planning, Strategy, and Risk was designated as the system owner.[5]

The eGRC Cloud System supports the following use cases:

- Audit Management: Tracking of FHFA audit assignment planning and status, document and meeting requests, audit reporting, and observations.
- Findings and Issues Management: Tracking of audit findings and remediation activities, verification of corrective actions, and risk exceptions and acceptance.
- Hotline Complaints: Tracking of hotline referrals from OIG, which are forwarded to the OPPR mailbox.
- Control Assurance and Governance: Maintenance of the risk and control matrix, control assessments, findings, reporting, and remediation tracking.
- Enterprise Risk Management: Maintenance of risk identification and assessments, risk profiles, and mitigation activities tracking.

FHFA's Security Responsibilities for the eGRC Cloud System

As delineated in the contractor's customer responsibility matrix (CRM), the contractor and FHFA share the responsibility for security of the eGRC Cloud System. The contractor is responsible for protecting the infrastructure that runs all the services offered in the contractor's cloud environment. FHFA is responsible for, among other things, the following five security controls as outlined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organization*:

- Access Control – defined as the safeguards used to grant or deny specific requests for obtaining and using information.
- Data Protection – defined as the safeguards used to identify, classify, securely handle, retain, and dispose of data.

[4] A pre-production environment as a non-production environment used to develop, integrate, and test features and system changes before they are deployed in the production environment.

[5] NIST defines a system owner as an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system. Additionally, NIST states the system owner is responsible for addressing the operational interests of the user community (i.e., users who require access to the system to satisfy mission, business, or operational requirements) and for ensuring compliance with information security requirements.

- Assessment, Authorization and Monitoring – defined as the measures used to assess whether security controls are implemented correctly and operating as intended, system authorizations are based on acceptable levels of risk, and common controls for inheritance by organizational systems are used.

- Identification and Authentication – defined as the safeguards used to uniquely identify organizational users and devices, verify claimed identities, protect passwords, and enforce strong authentication mechanisms prior to granting system access.

- Audit and Accountability – defined as safeguards used to create, protect, retain and review system audit records; track user and system activities; and monitor and analyze events for indicators of inappropriate or unusual activity.

Federal Standards and FHFA Requirements for Information Security

FISMA requires agencies to develop, report, and implement agency-wide programs to provide security for the information and information systems that support the operations and assets of the agency. In addition, FISMA requires agencies to implement periodic testing and evaluation of the effectiveness of their security policies, procedures, and practices. Pursuant to FISMA, the NIST prescribes standards and guidelines pertaining to federal information systems. Those standards provide minimum information security requirements necessary to improve the security of federal information and information systems. In addition, NIST develops and issues recommendations and guidance in SP documents.

FHFA governs the implementation and assessment of security controls for its information systems through policies, standards, plans, and procedures. These documents address areas such as access control, data protection, assessment, authorization, and monitoring, identification and authentication, and audit and accountability.

OBJECTIVE AND SCOPE .....

The objective of our audit was to determine whether FHFA effectively designed and implemented security controls for its eGRC Cloud System to manage access and protect information in accordance with federal standards and FHFA requirements from May 2025 through May 2026.

RESULTS

We determined that FHFA**'s** design and implementation of select security controls were not fully effective for its eGRC Cloud System to manage access and protect information in accordance with federal standards and FHFA requirements. While FHFA designed and implemented some of the security controls, we found weaknesses in other controls.

FHFA effectively designed and implemented controls that required:

- approvals when creating information system accounts and configured user groups in accordance with the principle of least privilege;
- performance of a comprehensive security control assessment for the production environment;
- enforcement of multifactor authentication (MFA) in the production environment; and
- review of audit logs for indicators of inappropriate or unusual activity in the production environment.

However, we identified weaknesses in all five NIST control areas that we tested. Specifically, we found that FHFA did not:

- consistently implement access controls for privileged and inactive accounts;
- document and consistently implement data protection controls for sanitizing identifying information from hotline complaints referred by the OIG;
- fully describe the controls applicable to the eGRC Cloud System in the security documentation;
- fully implement identification and authentication controls to: protect privileged account passwords, enforce MFA, and uniquely identify users, including contractors; and
- implement audit log procedures in the pre-production environment.

These weaknesses reduce FHFA's ability to ensure that access is appropriate, hotline complaint information is protected, and security controls are documented. As described below, we are reporting five findings.

Finding 1: FHFA Did Not Consistently Implement Access Controls for Privileged and Inactive Accounts

FHFA designed access controls for the eGRC Cloud System to manage user access and protect information. However, FHFA did not implement certain access controls consistently as designed. Specifically, we found that:

- FHFA did not limit the use of privileged accounts to the minimum access necessary to perform assigned duties. Three privileged users, including one contractor, were assigned system administrator roles but did not have corresponding non-privileged user accounts. These users accessed the system using their privileged accounts, including when they performed activities that did not require elevated privileges. For example, the contractor's privileged account provided privileged access to hotline complaint records in the production environment. Our review of access history logs found that this contractor and another contractor, who previously had privileged access to the system, accessed hotline complaint records using their privileged accounts.

- FHFA did not disable inactive user accounts within 35 days of inactivity. We reviewed eGRC Cloud System user accounts that were active and showed last login date of March 25, 2026, or earlier, and found 19 of 55 enabled user accounts (approximately 35 percent) were not disabled after 35 days of inactivity. Of the 19 user accounts, 11 user accounts were never logged into or had no recorded login activity within the system.

NIST SP 800-53 Rev. 5 requires that organizations provide users only the minimum access necessary to perform assigned duties, privileged accounts be used only for security-related activities, and inactive accounts are disabled after an organizationally defined period. The CRM places responsibility on customers to review and disable inactive accounts after 35 days.

OCFO management stated that eGRC Cloud System contractors required the system administrator role because they possess the technical skills and ability to perform system fixes and maintenance, including performing these functions on the complaints module, and that role is how configuration changes were made in the system. Contractors accessed the hotline complaint records in the production environment to resolve configuration and access issues. OCFO management also stated that during system implementation, privileged users were not assigned non-privileged accounts due to project workflow and troubleshooting requirements. According to OCFO management, the eGRC Cloud System relies on enterprise directory services to determine whether privileged user accounts remain active rather than using the cloud system's application-level inactivity. However, we found that an eGRC Cloud System account remains active as long as the associated enterprise directory account is active, even if the user has never logged into the application. As a result, accounts inactive for more than 35 days at the application level were not identified or disabled as required.

Due to the identified weaknesses, FHFA faces an increased risk of unauthorized access to sensitive system information. The Agency's implementation of the system administrator role permits access to hotline complaint records, as demonstrated by the two contractors who accessed these records. Further, the use of privileged accounts for tasks that do not require elevated permissions increases the risk of accidental or unauthorized configuration changes. Additionally, retaining 19 inactive user accounts increases the attack surface of the system.

Recommendations

We recommend the eGRC System Owner:

1. 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 NIST SP 800-53.

2. Review the 19 inactive user accounts on the eGRC Cloud System and determine if they should be disabled in accordance with NIST SP 800-53.

3. 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 NIST SP 800-53.

Finding 2: FHFA Did Not Document and Consistently Implement Data Protection Controls for Sanitizing Hotline Complaint Information

FHFA designed a process to remove identifying information from hotline complaints before personnel enter them into eGRC Cloud System, and we observed OCFO personnel perform this process. When FHFA receives a hotline complaint referral from OIG, an OCFO staff member saves the complaint in a folder on FHFA's network.[6] The staff member then sanitizes the complaint for personally identifiable information while entering it into the eGRC Cloud System. However, FHFA has not documented this process. Additionally, FHFA did not consistently implement this process because we found that identifying information remained in hotline complaint records after OCFO personnel completed the sanitization process. We reviewed 199 hotline complaint records in the production environment. Two of these records contained enough information for us to identify individuals named in the hotline complaints. One record included an individual's title and organization name, and the other record included an individual's last name, title, and current and former employers. We also reviewed hotline complaint information stored in the pre-production environment. We found two hotline complaint records with sensitive information in the pre-production environment. While one record was fully

[6] According to OCIO officials, the original hotline complaint record received from OIG is stored in a secure directory that has restricted access outside of the eGRC Cloud System.

sanitized, the other one was the same unsanitized record identified above that contained enough information for us to identify the individual named in the hotline complaint.

The Government Accountability Office's S*tandards for Internal Control in the Federal Government* (Green Book), Principle 11.07, requires that management design general control activities to mitigate information security risks. This includes documenting procedures to ensure that sensitive information is protected from unauthorized access, disclosure, or modification. Additionally, NIST SP 800-53 Rev. 5 requires organizations to protect the confidentiality of organization defined information at rest.

OCFO officials stated that hotline complaint information received from the OIG is protected through sanitization when it is entered into the system. The sanitization, review and preparation of hotline complaint information occur before being entered into the system, and this process was not included in system-specific documentation. However, when we asked an OCFO official to demonstrate this process, we observed that hotline complaints were being sanitized directly from the source records while entering them into the system. The eGRC System Owner acknowledged that the sanitization process was not included in the system-specific documentation but stated that OCFO could update their user guide to include this process.

In addition, OCFO officials stated that the pre-production environment does not process FHFA business data. When we asked why two records were stored in the pre-production environment, an OCFO official explained that two hotline complaints were entered to test how to generate a report listing of hotline complaints within the system. However, our review indicated that this task could have been completed using test or dummy data.

By not documenting and consistently implementing the hotline complaint sanitization process, identifying information was inadvertently entered into the production and pre-production environments, which increases the risk of unauthorized access and disclosure by those who may not have a need to know. Additionally, as noted in Finding 1, system administrators are permitted access to all hotline complaint records within the eGRC Cloud System. The unauthorized disclosure of this information could potentially cause harm to the identified individuals, damage the reputation of the Agency, and undermine trust in the hotline complaint management process.

Recommendations

We recommend the eGRC System Owner:

4. Document procedures for sanitizing hotline complaint records when entering them into the system to ensure sensitive information is not included.

5. Fully sanitize the two hotline complaint records that contain sensitive information in accordance with NIST SP 800-53.

6. Remove the two hotline complaint records that were transferred to the pre-production environment in accordance with NIST SP 800-53.

Finding 3: FHFA Did Not Fully Document the Security Controls as Part of the Assessment and Authorization Process

FHFA designed and implemented assessment, authorization, and monitoring controls for the eGRC Cloud System in accordance with federal requirements. However, FHFA did not fully describe the security controls that applied to the eGRC Cloud System production and pre-production environments. Specifically, we found that:

- FHFA's security documentation did not fully describe the controls applicable to the eGRC Cloud System. Furthermore, FHFA's eGRC Cloud System Customer Controls, Revision 1.3, states that it serves in place of the system security and privacy plan (SSPP). However, this document did not describe 87 of 92 controls that FHFA was responsible for implementing in the production environment. It also did not describe the security controls for the pre-production environment or identify the controls inherited from the FHFA SSPP for the General Support System (GSS), Version 3.4 (October 22, 2025) and the FHFA Common Control Plan, Version 3.8 (November 3, 2025).

- FHFA's SSPP did not identify the system's name, security categorization, impact level, operational status, system type, authorizing official, system environment, and security authorization boundary.

NIST SP 800-53 Rev. 5 requires organizations to provide an overview of the security and privacy requirements for the system and describe the controls in place or planned for meeting the security and privacy requirements. Furthermore, NIST SP 800-18 Revision 2, *Guide for Developing Security Plans for Federal Information Systems,* requires that SSPPs identify the system's name, security categorization, impact level, operational status, system type, and authorizing official. It also requires that the SSPP describes the system's environment, security authorization boundary, and how security controls are implemented or planned to be implemented.

OCFO management stated that the eGRC Cloud System Customer Controls document is not intended to serve as FHFA's full SSPP or as a comprehensive record of all required controls. According to OCFO management, FHFA follows a control structure in which the implementation of a majority of the controls are inherited from the FHFA GSS and the FHFA Common Control Plan. Most of the controls assigned to FHFA in the CRM are not designated as

system specific controls for the eGRC Cloud System. Accordingly, the eGRC Cloud System Customer Controls document only describes a small subset of controls that require direct configuration, operation, or workflow execution within the system to prevent duplicative documentation of controls already fully implemented and assessed at the enterprise level. However, we noted the eGRC Cloud System Customer Controls document explicitly states that it serves in place of a SSPP, yet it did not include any information on the implementation of inherited controls from the FHFA SSPP for the GSS or the FHFA Common Control Plan. Additionally, the eGRC Cloud System Customer Controls document did not describe the full subset of system specific controls as noted above.

These documentation gaps increase the risk that security weaknesses remain undetected and are not remediated in a timely manner. They also limit FHFA's visibility into whether security controls are appropriately implemented and operating effectively across all system environments.

Recommendation

We recommend the eGRC System Owner:

7. Update the eGRC Cloud System Customer Controls document in accordance with NIST SP 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 SSPP for the GSS 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.

Finding 4: FHFA Did Not Fully Implement Identification and Authentication Controls

FHFA designed and implemented certain identification and authentication controls for the eGRC Cloud System. For example, MFA was enforced in the production environment. However, FHFA did not fully implement the controls that we tested in the production and pre-production environments. Specifically, we found that:

- FHFA did not consistently protect a privileged account password in the pre-production environment. During our review, we found a system administrator's password was

stored in plaintext. The password also did not meet FHFA's password strength requirements. OCFO management attributed this to human error.

- FHFA did not enforce MFA in the pre-production environment. We found that users could authenticate with only a username and password. When we asked OCFO management why MFA was not enforced, a reason was not provided.

- FHFA did not uniquely associate certain pre-production accounts with individual users. Of the 56 user accounts we reviewed, 12 user accounts had generic test names and were not associated with unique system users. OCFO management stated that these accounts do not authenticate through FHFA's enterprise directory services and therefore did not inherit unique identity attributes. Vendor documentation, however, identifies functionality that allows FHFA to add or modify account information, including unique identity attributes.

- FHFA did not identify a contractor account in the production and pre-production environment. Based on our review of the eGRC Cloud System user accounts, we found that an active contractor account did not contain identifiers or other information distinguishing them from other eGRC Cloud System user accounts. OCFO management stated contractor identifiers from FHFA's enterprise directory services do not transfer to the eGRC Cloud System during the account authentication process. Vendor documentation, however, identifies functionality that allows FHFA to add or modify account information, including contractor identifiers.

NIST SP 800-53 Rev. 5 requires organizations to protect passwords from unauthorized disclosure, implement MFA for users, and uniquely identify each user by assigning distinct individual identifiers. The CRM states that FHFA is responsible for uniquely identifying contractors when creating identifiers in the application.

Storing plaintext passwords to privileged accounts could lead to data exposure and compromise of the pre-production environment. By not enforcing MFA on the pre-production environment, attackers can more easily use stolen, brute-forced, or phished credentials to take over accounts, gain initial access, and potentially pivot into production systems. Additionally, the absence of identifiers further weakens monitoring and accountability by making it difficult to associate actions with specific individuals. Furthermore, not including characteristics that uniquely identify contractors weakens monitoring controls related to access control and data handling within the eGRC Cloud System.

Recommendations

We recommend the eGRC System Owner:

8. 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.

9. Enable and enforce MFA for access to the pre-production environment in accordance with NIST SP 800-53.

10. 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 NIST SP 800-53.

11. Ensure that the contractor account includes unique identifiers in accordance with the CRM.

Finding 5: FHFA Did Not Implement Audit Log Procedures for the Pre-Production Environment

FHFA designed procedures to review eGRC Cloud System audit logs and fully implemented these procedures in the production environment. However, we found that FHFA did not implement those procedures in the pre-production environment. Specifically, FHFA did not review and analyze audit logs for indications of inappropriate or unusual activity in the pre-production environment.

NIST SP 800-53 Rev. 5 requires that agencies review and analyze system audit records for indications of inappropriate or unusual activity. FHFA's eGRC Cloud System Customer Controls document states that the eGRC System Owner will review the security events log for any suspicious or unusual activity as needed and on a quarterly basis. This document does not distinguish between the production and pre-production environments or state that this is only applicable to the production environment.

OCFO management stated that FHFA's quarterly audit log review procedures focus on the production environment, where FHFA data resides and mission operations occur. Furthermore, because the pre-production environment contains only configuration and test data and no official FHFA records, it was not included in their audit review, analysis, and reporting on operational monitoring cycle. According to OCFO management, the pre-production environment is a non-operational environment in which the pre-production and production environments are logically separated. However, as noted in Finding 2, hotline complaint referral data was entered into the pre-production environment.

By not reviewing the security events log for the pre-production environment, FHFA is at an increased risk that malicious activity that may occur remains undetected. As such, FHFA may not identify and/or respond to potential security incidents or unauthorized activity.

Recommendation

We recommend the eGRC System Owner:

12. Ensure that audit logs for the pre-production environment are reviewed as needed or on a quarterly basis in accordance with the eGRC Cloud System Customer Controls document and NIST SP 800-53.

FHFA COMMENTS AND OIG EVALUATION.....

We provided FHFA management with an opportunity to review and provide technical comments to a draft of this audit report. We considered those comments in finalizing this report.

In a written response, FHFA management acknowledged receipt of this report and stated that it identified concerns regarding the accuracy of some information presented. In addition, management reported taking initial actions to address some recommendations and is assessing the benefits of implementing others while considering compensating controls it described as already in place. The response also stated that OIG did not provide the additional time requested to fully review the report, and management was unable to provide a comprehensive response to the recommendations due to fiscal year-end priorities. Management plans to provide an update on corrective actions completed and its decision on whether to implement the remaining recommendations by November 30, 2026.

We evaluated FHFA's management response and found no specificity of report inaccuracies or additional evidence supporting management's general accuracy concerns. The response provided no basis for further changes to our findings or recommendations, and accordingly, no changes were made. Management also did not express agreement or disagreement with our recommendations or describe the reported initial actions and compensating controls for us to assess whether they address the identified weaknesses. As such, management's response did not address our recommendations. The recommendations will remain open until FHFA has implemented corrective actions that we can confirm sufficiently address them. FHFA's written response, in its entirety, is included in Appendix II of this report.

APPENDIX I: METHODOLOGY

To accomplish our objective, we performed the following procedures:

- Reviewed Government Accountability Office's *Standards for Internal Control in the Federal Government* (GAO-25-107721; May 2025), applicable during the audit scope, and determined that the design control activities component was significant to this objective. We focused on the underlying principle that management should: (1) design appropriate types of general control activities to mitigate information security risks, and (2) design logical and physical access control activities including restricting access or detecting inappropriate access to information and information technology.
- Reviewed the following NIST publications:
  - NIST SP 800-18, Revision 2, *Guide for Developing Security Plans for Federal Information Systems* (June 30, 2026)
  - NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (updated December 10, 2020)
- Reviewed the following FHFA policies and procedures to determine FHFA's security controls and process for access controls, control activities, identification and authentication controls, assessment, authorization and monitoring controls, and audit and accountability controls:
  - eGRC Cloud System Customer Controls, Revision 1.3 (April 22, 2026)
  - FHFA Access Control Standard, Revision 2.4 (October 6, 2025)
  - FHFA Assessment and Authorization Plan, Revision 4.2 (September 30, 2025)
  - FHFA Common Control Plan, Version 3.8 (November 3, 2025)
  - FHFA Identification and Authentication Standard, Revision 2.3 (October 20, 2025)
  - FHFA Information Security Continuous Monitoring Strategy, Revision 3.7 (October 24, 2025)
  - FHFA System and Communications Protection Standard, Revision 2.4 (October 26, 2025)
  - FHFA System Security and Privacy Plan for the General Support System, Version 3.4 (October 22, 2025)

- Obtained, reviewed, and analyzed the eGRC Cloud System authorization and assessment documentation including the Security Assessment Report, Control Assessment Plan, Control Assessment, and CRM for security controls that FHFA is responsible for as a customer or has shared responsibility in implementing.
- Reviewed the 18 Center for Internet Security Critical Security Controls to identify the following key risk areas that impact cloud systems:
    - Access Controls
    - Data Protection controls
    - Account Management controls
    - Audit Log Management controls
- Obtained, reviewed, and analyzed FHFA's eGRC Cloud System documentation to assess the design and implementation of select security controls required by NIST SP 800-53 and the CRM in the following areas:
    - Access Controls
    - Data Protection controls
    - Assessment, Authorization, and Monitoring controls
    - Identification and Authentication controls
    - Audit and Accountability controls
- Assessed the design and implementation of the select security controls through interviews, walkthroughs, observations, and review of system generated information. Our procedures included reviewing account information, hotline complaint records, authentication settings, audit logs, and other relevant information from the production and pre-production environments.
- Identified the population of 199 hotline complaint records stored on the eGRC Cloud System production environment and reviewed these records to determine whether identifying information remained after FHFA's sanitization process.
- Interviewed OCFO and Office of Chief Information Officer officials and staff.

We conducted this performance audit between March 2026 and September 2026, at our headquarters in Washington, D.C., 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

KRISTIN SALZER

Digitally signed by KRISTIN SALZER
Date: 2026.09.21 16:23:21 -04'00'

FROM: Edom Aweke, Chief Financial Officer, Office of Chief Financial Officer

SUBJECT: Audit Report: *FHFA's Design and Implementation of Select Security Controls for its eGRC Cloud System Were Not Fully Effective* (OA-26-006)

DATE: September 21, 2026

FHFA acknowledges receipt of the above-referenced Office of Inspector General draft report (Report). Based on the Agency's preliminary review of the Report, management identified concerns regarding the accuracy of some information presented in the Report. Management has taken initial actions to address some of the recommendations and is assessing the benefits of implementing others while considering compensating controls that are already in place. OIG did not provide the additional time that management requested to conduct the necessary due diligence to fully review the Report. Given the fiscal year-end priorities, management is unable to prepare a comprehensive response to these recommendations at this time.

In accordance with Office of Management and Budget Circular A-50, *Audit, Inspection, or Evaluation Follow-Up*, management will provide an update on corrective actions completed to date and its decision on whether to implement the remaining recommendations by November 30, 2026.

If you have any questions related to this response, please contact Ivan Bengtson.

cc: John Major
Jeff Harris

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